

Simultaneous Partial Inverses and Decoding Interleaved Reed-Solomon Codes

Jiun-Hung Yu and Hans-Andrea Loeliger

Abstract—This paper introduces the simultaneous partial-inverse problem for polynomials and develops its application to decoding interleaved Reed-Solomon codes and subfield-evaluation codes beyond half the minimum distance. The simultaneous partial-inverse problem has a unique solution (up to a scale factor), which can be computed by an efficient new algorithm, for which we also offer some variations. Decoding interleaved Reed-Solomon codes and subfield-evaluation codes (beyond half the minimum distance) can be reduced to the simultaneous partial-inverse problem, and pertinent decoding algorithms are obtained by easy adaptations of the simultaneous partial-inverse algorithms. The resulting unique-decoding algorithms are new and efficient, and they have state-of-the-art decoding capability.

Index Terms—Interleaved Reed-Solomon codes, subfield-evaluation codes, simultaneous partial-inverse problem, simultaneous partial-inverse algorithm, generalized Euclidean algorithm, multi-sequence Berlekamp–Massey algorithm.

I. INTRODUCTION

This paper revolves around the following problem and develops its application to decoding interleaved Reed-Solomon codes and subfield-evaluation codes beyond half the minimum distance.

Simultaneous Partial-Inverse (SPI) Problem: For $i = 1, \dots, L$, let $b^{(i)}(x)$ and $m^{(i)}(x)$ be nonzero polynomials over some field F with $\deg b^{(i)}(x) < \deg m^{(i)}(x)$. For fixed $\tau^{(i)} \in \mathbb{Z}$ with $0 \leq \tau^{(i)} \leq \deg m^{(i)}(x)$, find a nonzero polynomial $\Lambda(x) \in F[x]$ of the smallest degree such that

$$\deg(b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x)) < \tau^{(i)} \quad (1)$$

for all $i \in \{1, \dots, L\}$. \square

We will see that this problem has always a unique solution (up to a scale factor), and the solution satisfies

$$\deg \Lambda(x) \leq \sum_{i=1}^L \left(\deg m^{(i)}(x) - \tau^{(i)} \right). \quad (2)$$

In the special case where $L = 1$, the SPI problem reduces to the partial-inverse problem in [3], [4], which includes Padé approximation and various key equations for decoding Reed-Solomon codes and some related codes [4]. In this case, the SPI algorithms that will be proposed in this paper reduce to the corresponding partial-inverse algorithms in [4]. However, the generalization from $L = 1$ to $L > 1$ is not obvious.

For $L > 1$, the simultaneous partial-inverse problem is similar to the multi-sequence shift-register synthesis (MSSRS)

problem [5], [6], and it can be used for similar purposes (such as in [7]–[10]). However, the simultaneous partial-inverse problem is not identical to the MSSRS problem of [5], [6]: e.g., neither the original LFSRS problem [11] nor the MSSRS problem of [5], [6] have always a unique solution, and the degree bound (2) does not apply to them. In this paper, uniqueness of the solution and the degree bound (2) will play an important role throughout.

The codes in this paper are of the following type. Let $F = F_q$ be a finite field with q elements. We will consider codes where codewords are $L \times n$ arrays over F such that each row is a codeword from some (n, k) Reed-Solomon code. We will only consider column errors, and we will not distinguish between columns with a single error and columns with many errors.

The Reed-Solomon code for each row is defined as follows. Let $\beta_0, \dots, \beta_{n-1}$ be n different elements of F . The (n, k) code is then defined as the set

$$\{(a(\beta_0), \dots, a(\beta_{n-1})) : a(x) \in F[x] \text{ with } \deg a(x) < k\}. \quad (3)$$

Note that such codes include both shortened and singly-extended Reed-Solomon codes. The generalization to the case where the row codes have different dimensions k is developed in Appendix A.

It is well known [8], [12], [13] that such interleaved Reed-Solomon codes can equivalently be viewed as shortened Reed-Solomon codes over F_{q^L} simply by replacing $F[x] = F_q[x]$ in (3) by $F_{q^L}[x]$ while the evaluation points $\beta_0, \dots, \beta_{n-1}$ remain in F_q . Note that symbol errors in F_{q^L} correspond to column errors in the array code.

Decoding such subfield-evaluation codes beyond the Guruswami-Sudan decoding radius [14] was pioneered in [7], [12], [13], [15], and decoding interleaved Reed-Solomon codes beyond half the minimum distance has been much advanced in [8], [10], [16]–[18]. Note that some of these papers use list-decoding algorithms [13]–[15], while others use unique-decoding algorithms that return at most one codeword [7], [8], [10], [12], [16]–[18]. The best unique-decoding algorithms can now correct t errors (column errors or F_{q^L} -symbol errors) up to the radius

$$t \leq \frac{L}{L+1}(n-k) \quad (4)$$

with high probability if q is large [7], [8].

In this paper, we reduce the decoding of such codes (in more than one way) to a simultaneous partial-inverse problem. The resulting decoding algorithms will be shown to have state-of-the-art decoding capability.

Both authors are with the Dept. of Information Technology and Electrical Engineering, ETH Zurich, CH-8092 Zürich, Switzerland.

This paper was presented in part at Allerton 2014 [1] and at ISIT 2015 [2].

This paper is similar in structure to its companion paper [4]. By developing the decoding problem from a new starting point—the simultaneous partial-inverse problem—we gain generality and clarity, we unify and improve results from different approaches in the literature, and we obtain many novelties in detail.

First, we will investigate the simultaneous partial-inverse problem without regard to any algorithm, and we will find many properties of it that will be helpful for decoding later on. In particular, we prove uniqueness of the solution and the degree bound (2), and we discuss irrelevant coefficients in $b^{(i)}(x)$ and $m^{(i)}(x)$ (and how to get rid of them). We also show that the simultaneous partial-inverse problem for general $m^{(i)}(x)$ can be transformed into a simultaneous partial-inverse problem with $m^{(i)}(x) = x^\nu$. This transform permits us to show that the SPI problem for general $m^{(i)}(x)$ can be solved with the same complexity as for $m^{(i)}(x) = x^\nu$.

Second, we develop efficient algorithms to solve the simultaneous partial inverse problem. We first give a basic algorithm, which generalizes the basic algorithm in [4] to $L > 1$. In some special cases (including $m^{(i)}(x) = x^\nu$, $m^{(i)}(x) = x^\nu - 1$, and $m^{(i)}(x) = x^\nu - x$), this algorithm looks very much like, and is as efficient as, the MSSRS algorithm in [6] (see also [19]). (Note that the case $m^{(i)}(x) = x^\nu - x$ is essential for singly extended Reed-Solomon codes). We then note that this algorithm is easily translated into two further algorithms; both of them are new, but one of them is quite similar to a generalized Euclidean algorithm for the MSSRS problem [5] (see also [9]). For $L = 1$, the three SPI algorithms reduce to the corresponding partial-inverse algorithms in [4].

Third, we show that decoding interleaved Reed-Solomon codes (and subfield evaluation codes) can be reduced rather naturally to a simultaneous partial-inverse problem, and decoded by easy adaptations of the SPI algorithms in Section IV. The resulting algorithms are very efficient and are guaranteed to correct t (column-) errors up to the radius

$$t \leq \frac{n - k + r_E - 1}{2} \quad (5)$$

where r_E is the rank of the error matrix $E \in F^{L \times n}$ that corrupts the transmitted (array-) codeword.

Note that (5) agrees with the best prior bound as in [10] (but our algorithms do not require the computation of r_E and are therefore more efficient). Note also that (5) is strictly better than the guarantee in [8] by a margin of $r_E/2$; if $r_E = t$ (which is very likely if $t \leq L$), then (5) reduces to

$$t < n - k, \quad (6)$$

(cf. Proposition 7 with $t = |U_E|$).

Fourth, we complement the bound (5) by

$$P_f < \frac{q^{-L(n-k)+(L+1)t}}{q-1} \quad (7)$$

where P_f is the probability of decoding failure for random errors, i.e., the t nonzero columns of the error pattern are uniformly distributed over $F_q^L \setminus \{0\}$ (see Theorem 6). Note that (7) implies that errors can be corrected (with high probability, if q is large) up to the radius (4).

The bound (7) almost agrees with, but is strictly better than, the best prior bound of [8], and it beats the bound of [7]. The small, but positive, advantage over the bound of [8] appears to depend essentially on the partial-inverse approach. Moreover, our proof of (7) is shorter than the proof of the bound in [8].

We will see that the proposed decoding algorithms are very efficient even if L is large (cf. Propositions 6 and 7). We also note that, in contrast to the prior literature [8], [10], the set $\{\beta_0, \dots, \beta_{n-1}\}$ of evaluation points is allowed to contain 0.

In Appendix A, we generalize these algorithms to array codes where the row codes can have different dimension k , and we obtain satisfactory generalizations of (4)–(7). (Applications of such codes can be found, e.g., in [8], [20].)

The paper is structured as follows. The basic properties of the simultaneous partial-inverse problem are given in Section II. Two general methods to simplify the original problem are addressed in Section III. The basic SPI algorithm, and two variations of it, are given in Section IV. In Section V, we establish notation and review some basic concepts for decoding interleaved Reed-Solomon codes. The actual decoding algorithms are given in Section VI, and their decoding capabilities are analyzed in detail in Section VII. The proof of the basic SPI algorithm is given in Section VIII, and Section IX concludes the main part of the paper. In Appendix A, we generalize the results to array codes with row codes of different dimensions.

We will use the following notation. The coefficient of x^d of a polynomial $b(x) \in F[x]$ will be denoted by b_d , and the leading coefficient (i.e., the coefficient of $x^{\deg b(x)}$) of a nonzero polynomial $b(x)$ will be denoted by $\text{lcf } b(x)$, and we also define $\text{lcf}(0) \triangleq 0$. We will use “mod” both as in $r(x) = b(x) \bmod m(x)$ (the remainder of a division) and as in $b(x) \equiv r(x) \bmod m(x)$ (a congruence modulo $m(x)$).

II. BASIC PROPERTIES OF THE SIMULTANEOUS PARTIAL-INVERSE PROBLEM

The simultaneous partial-inverse problem as defined in Section I has the following properties, which we will need later on.

Proposition 1. The simultaneous partial-inverse problem has always a solution. \square

Proof: The polynomial $\Lambda(x) = m^{(1)}(x) \cdots m^{(L)}(x)$ satisfies $b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x) = 0$ for all i , which implies the existence of a solution for any $\tau^{(i)} \geq 0$. \blacksquare

Proposition 2. The solution $\Lambda(x)$ of a simultaneous partial-inverse problem is unique up to a scale factor $\in F$. \square

Proof: Let $\Lambda'(x)$ and $\Lambda''(x)$ be two solutions of the problem, which implies $\deg \Lambda'(x) = \deg \Lambda''(x) \geq 0$. Define

$$r'^{(i)}(x) \triangleq b^{(i)}(x)\Lambda'(x) \bmod m^{(i)}(x) \quad (8)$$

$$r''^{(i)}(x) \triangleq b^{(i)}(x)\Lambda''(x) \bmod m^{(i)}(x) \quad (9)$$

and consider

$$\Lambda(x) \triangleq \left(\text{lcf } \Lambda''(x) \right) \Lambda'(x) - \left(\text{lcf } \Lambda'(x) \right) \Lambda''(x). \quad (10)$$

Then

$$\begin{aligned} r^{(i)}(x) &\triangleq b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x) \\ &= \left(\text{lcf } \Lambda''(x)\right)r'^{(i)}(x) - \left(\text{lcf } \Lambda'(x)\right)r''^{(i)}(x) \end{aligned} \quad (11)$$

by the natural ring homomorphism $F[x] \rightarrow F[x]/m^{(i)}(x)$. Clearly, (12) implies that $\Lambda(x)$ also satisfies (1) for every $1 \leq i \leq L$. But (10) implies $\deg \Lambda(x) < \deg \Lambda'(x)$, which is a contradiction unless $\Lambda(x) = 0$. Thus $\Lambda(x) = 0$, which means that $\Lambda'(x)$ equals $\Lambda''(x)$ up to a scale factor. \square

Proposition 3 (Degree Bound). If $\Lambda(x)$ solves the simultaneous partial-inverse problem, then

$$\deg \Lambda(x) \leq \sum_{i=1}^L \left(\deg m^{(i)}(x) - \tau^{(i)} \right). \quad (13)$$

Proof: The case $\tau^{(i)} = \deg m^{(i)}(x)$ for all i is obvious. Otherwise, let $\nu_i \triangleq \deg m^{(i)}(x) - \tau^{(i)}$ and $\nu \triangleq \sum_{i=1}^L \nu_i$, and consider, for $i = 1, \dots, L$, the linear mappings

$$\varphi_i : F^{\nu+1} \rightarrow F^{\nu_i} \quad (14)$$

given by

$$(\Lambda_0, \dots, \Lambda_\nu) \mapsto \Lambda(x) \triangleq \Lambda_0 + \Lambda_1 x + \dots + \Lambda_\nu x^\nu \quad (15)$$

$$\mapsto r^{(i)}(x) \triangleq b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x) \quad (16)$$

$$\mapsto (r_0^{(i)}, \dots, r_{\deg m^{(i)}(x)-1}^{(i)}) \quad (17)$$

$$\mapsto (r_{\tau^{(i)}}^{(i)}, \dots, r_{\deg m^{(i)}(x)-1}^{(i)}). \quad (18)$$

Note that a polynomial $\Lambda_0 + \Lambda_1 x + \dots + \Lambda_\nu x^\nu$ satisfies (1) if and only if $(\Lambda_0, \dots, \Lambda_\nu) \in \ker \varphi_i$. But

$$\begin{aligned} \dim \left(\bigcap_{i=1}^L \ker \varphi_i \right) &\geq \nu + 1 - \sum_{i=1}^L \nu_i \\ &= 1 \end{aligned} \quad (19)$$

and $\left(\bigcap_{i=1}^L \ker \varphi_i \right)$ is not trivial. There thus exists some nonzero polynomial $\Lambda_0 + \Lambda_1 x + \dots + \Lambda_\nu x^\nu$ that satisfies (1) simultaneously for $i = 1, \dots, L$. \blacksquare

III. MORE ABOUT THE SIMULTANEOUS PARTIAL-INVERSE PROBLEM

A. Reduced Simultaneous Partial-Inverse Problem

Let

$$D \triangleq \sum_{i=1}^L \left(\deg m^{(i)}(x) - \tau^{(i)} \right), \quad (21)$$

cf. (13).

Proposition 4 (Irrelevant Coefficients). In the simultaneous partial-inverse problem, coefficients $b_\ell^{(i)}$ of $b^{(i)}(x)$ with

$$\ell < \tau^{(i)} - D \quad (22)$$

and coefficients $m_s^{(i)}$ of $m^{(i)}(x)$ with

$$s \leq \tau^{(i)} - D \quad (23)$$

have no effect on the solution $\Lambda(x)$. \square

Proof: From (22) and (13), we obtain

$$\ell + \deg \Lambda(x) < \tau^{(i)}, \quad (24)$$

which proves the first claim. As for the second claim, we begin by writing

$$b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x) = b^{(i)}(x)\Lambda(x) - m^{(i)}(x)q^{(i)}(x) \quad (25)$$

for some $q^{(i)}(x) \in F[x]$ with

$$\deg q^{(i)}(x) < \deg \Lambda(x). \quad (26)$$

(If $q^{(i)}(x) \neq 0$, (26) follows from considering the leading coefficient of the right-hand side of (25) with $\deg b^{(i)}(x) < \deg m^{(i)}(x)$). From (23), (26), and (13), we then obtain

$$s + \deg q^{(i)}(x) < \tau^{(i)}. \quad (27)$$

The second claim then follows from (25) and (27). \blacksquare

Irrelevant coefficients according to Proposition 4 may be set to zero without affecting the solution $\Lambda(x)$. In fact, such coefficients can be stripped off as follows:

Proposition 5 (Reduced SPI Problem). Consider a simultaneous partial-inverse problem as stated in Section I. If

$$s^{(i)} \triangleq \tau^{(i)} - D > 0, \quad (28)$$

define $\tilde{b}^{(i)}(x)$ and $\tilde{m}^{(i)}(x)$ with

$$\tilde{b}_\ell^{(i)} \triangleq b_{\ell+s^{(i)}}^{(i)} \quad (29)$$

and

$$\tilde{m}_\ell^{(i)} \triangleq m_{\ell+s^{(i)}}^{(i)} \quad (30)$$

for $\ell \geq 0$. Then the modified simultaneous partial-inverse problem with $b^{(i)}(x)$, $m^{(i)}(x)$, and $\tau^{(i)}$ replaced by $\tilde{b}^{(i)}(x)$, $\tilde{m}^{(i)}(x)$, and $\tilde{\tau}^{(i)} \triangleq \tau^{(i)} - s^{(i)}$, respectively, has the same solution $\Lambda(x)$ as the original simultaneous partial-inverse problem. In addition, we have

$$b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x) = \tilde{b}^{(i)}(x)\Lambda(x) \bmod \tilde{m}^{(i)}(x) \quad (31)$$

\square

Proof of Proposition 5: Consider an auxiliary simultaneous partial-inverse problem with $b^{(i)}(x)$ replaced by $x^{s^{(i)}}\tilde{b}^{(i)}(x)$ and $m^{(i)}(x)$ replaced by $x^{s^{(i)}}\tilde{m}^{(i)}(x)$ (and $\tau^{(i)}$ unchanged). This auxiliary problem has the same solution as the original problem by Proposition 4. The equivalence of this auxiliary problem with the modified problem is obvious from (25). \square

B. Monomialized Simultaneous Partial-Inverse Problem

Consider a simultaneous partial-inverse problem as stated in Section I, and let u be a positive integer that satisfies

$$u \geq \deg \Lambda(x) \quad (32)$$

where $\Lambda(x)$ is the solution of the problem. Moreover, let

$$n^{(i)} \triangleq \deg m^{(i)}(x). \quad (33)$$

The simultaneous partial-inverse problem (with general $m^{(i)}(x)$) can be transformed into another simultaneous partial-inverse problem where (1) is replaced by

$$\deg \left(\tilde{b}^{(i)}(x)\Lambda(x) \bmod x^{n^{(i)}-\tau^{(i)}+u} \right) < u \quad (34)$$

with $\tilde{b}^{(i)}(x)$ as defined below. The precise statement is given as Theorem 1 below. Note that we need the additional condition

$$\tau^{(i)} < n^{(i)}. \quad (35)$$

(The condition (35) does not entail any loss in generality: if $\tau^{(i)} = n^{(i)}$, then the two polynomials $b^{(i)}(x)$ and $m^{(i)}(x)$ can be removed from the original SPI problem (1) without affecting its solution).

The polynomial $\tilde{b}^{(i)}(x)$ in (34) is defined as follows. Let

$$\bar{b}^{(i)}(x) \triangleq x^{n^{(i)}-1} b^{(i)}(x^{-1}). \quad (36)$$

$$\bar{m}^{(i)}(x) \triangleq x^{n^{(i)}} m^{(i)}(x^{-1}). \quad (37)$$

Moreover, let $w^{(i)}(x)$ be the inverse of

$$\bar{m}^{(i)}(x) \bmod x^{n^{(i)}-\tau^{(i)}+u} \quad (38)$$

in ring $F[x]/x^{n^{(i)}-\tau^{(i)}+u}$; this inverse exists because $\bar{m}^{(i)}(0) \neq 0$, which implies that $\bar{m}^{(i)}(x)$ is relatively prime to $x^{n^{(i)}-\tau^{(i)}+u}$. Further, let

$$s^{(i)}(x) \triangleq (w^{(i)}(x) \bar{b}^{(i)}(x)) \bmod x^{n^{(i)}-\tau^{(i)}+u}, \quad (39)$$

and finally

$$\tilde{b}(x) \triangleq x^{n^{(i)}-\tau^{(i)}+u-1} s^{(i)}(x^{-1}). \quad (40)$$

Theorem 1 (Monomialized SPI Problem). Consider the simultaneous partial-inverse problem as stated in Section I with the additional condition (35), and let u be a positive integer satisfying (32) as defined above. Then the modified simultaneous partial-inverse problem where $b^{(i)}(x)$, $m^{(i)}(x)$, and $\tau^{(i)}$ are replaced by $\tilde{b}^{(i)}(x)$ (as defined above), $x^{n^{(i)}-\tau^{(i)}+u}$, and u , respectively, has the same solution $\Lambda(x)$ as the original simultaneous partial-inverse problem. In addition, we have

$$b^{(i)}(x) \Lambda(x) \operatorname{div} m^{(i)}(x) = \tilde{b}^{(i)}(x) \Lambda(x) \operatorname{div} x^{n^{(i)}-\tau^{(i)}+u} \quad (41)$$

□

Note that D as in (21) qualifies as u in (32). Note also that the computation of $\tilde{b}^{(i)}(x)$ requires the computation of $w^{(i)}(x)$ (= the inverse of (38) in $F[x]/x^{n^{(i)}-\tau^{(i)}+u}$), which can be computed by the extended Euclidean algorithm or by the algorithms in [4, Sec IV] (which coincide with the SPI algorithms of Section IV for $L = 1$).

Proof of Theorem 1: Consider the original SPI problem (1) and let $\Lambda(x)$ be its solution (which is unique up to a nonzero scale factor). Let

$$r^{(i)}(x) \triangleq b^{(i)}(x) \Lambda(x) \bmod m^{(i)}(x), \quad (42)$$

where $\deg r^{(i)}(x) < \tau^{(i)}$. We then write

$$r^{(i)}(x) = b^{(i)}(x) \Lambda(x) - q^{(i)}(x) m^{(i)}(x) \quad (43)$$

for some (unique) $q^{(i)}(x)$ with

$$\deg q^{(i)}(x) < \deg \Lambda(x) \leq u. \quad (44)$$

Now let

$$\bar{\Lambda}(x) \triangleq x^u \Lambda(x^{-1}) \quad (45)$$

$$\bar{q}^{(i)}(x) \triangleq x^{u-1} q^{(i)}(x^{-1}) \quad (46)$$

$$\bar{r}^{(i)}(x) \triangleq x^{\tau^{(i)}-1} r^{(i)}(x^{-1}). \quad (47)$$

By substituting x^{-1} for x in (43) and multiplying both sides by $x^{n^{(i)}+u-1}$ (i.e., reversing (43)), we obtain

$$x^{n^{(i)}+u-\tau^{(i)}} \bar{r}^{(i)}(x) = \bar{b}^{(i)}(x) \bar{\Lambda}(x) - \bar{q}^{(i)}(x) \bar{m}^{(i)}(x). \quad (48)$$

We then have

$$\bar{b}^{(i)}(x) \bar{\Lambda}(x) \equiv \bar{q}^{(i)}(x) \bar{m}^{(i)}(x) \bmod x^{n^{(i)}-\tau^{(i)}+u} \quad (49)$$

and therefore

$$w^{(i)}(x) \bar{b}^{(i)}(x) \bar{\Lambda}(x) \equiv \bar{q}^{(i)}(x) \bmod x^{n^{(i)}-\tau^{(i)}+u} \quad (50)$$

(where $w^{(i)}(x)$ as defined above is the inverse of $\bar{m}^{(i)}(x)$ in the ring $F[x]/x^{n^{(i)}-\tau^{(i)}+u}$) and thus

$$s^{(i)}(x) \bar{\Lambda}(x) \equiv \bar{q}^{(i)}(x) \bmod x^{n^{(i)}-\tau^{(i)}+u} \quad (51)$$

with $s^{(i)}(x)$ as defined in (39). Note that $\deg \bar{\Lambda}(x) \leq u$ and $\deg \bar{q}^{(i)}(x) < u$ from (44).

We now write (51) as

$$s^{(i)}(x) \bar{\Lambda}(x) = \bar{p}^{(i)}(x) x^{n^{(i)}-\tau^{(i)}+u} + \bar{q}^{(i)}(x) \quad (52)$$

for some (unique) $\bar{p}^{(i)}(x)$ with $\deg \bar{p}^{(i)}(x) < \deg \bar{\Lambda}(x) \leq u$, and let

$$p^{(i)}(x) \triangleq x^{u-1} \bar{p}^{(i)}(x^{-1}). \quad (53)$$

By substituting x^{-1} for x in (52) and multiplying both sides by $x^{n^{(i)}-\tau^{(i)}+2u-1}$, we obtain

$$\tilde{b}^{(i)}(x) \Lambda(x) = x^{n^{(i)}-\tau^{(i)}+u} q^{(i)}(x) + p^{(i)}(x), \quad (54)$$

from which we have

$$\deg(\tilde{b}^{(i)}(x) \Lambda(x) \bmod x^{n^{(i)}-\tau^{(i)}+u}) < u. \quad (55)$$

We have arrived at the modified SPI problem.

Now, let $\tilde{\Lambda}(x)$ denote the solution of the modified SPI problem; clearly

$$\deg \tilde{\Lambda}(x) \leq \deg \Lambda(x). \quad (56)$$

In the following, we will show that

$$\deg \tilde{\Lambda}(x) \geq \deg \Lambda(x), \quad (57)$$

Then from (56) and (57), we have $\deg \tilde{\Lambda}(x) = \deg \Lambda(x)$. We can then conclude from Proposition 2 that $\Lambda(x)$ solves the modified SPI problem; (41) is then obvious from (54).

It remains to prove (57). We begin by writing that

$$\deg(\tilde{b}^{(i)}(x) \tilde{\Lambda}(x) \bmod x^{n^{(i)}-\tau^{(i)}+u}) < u \quad (58)$$

with $\deg \tilde{\Lambda}(x) \leq u$ because of (56). Now, let

$$\tilde{p}^{(i)}(x) \triangleq \tilde{b}^{(i)}(x) \tilde{\Lambda}(x) \bmod x^{n^{(i)}-\tau^{(i)}+u}, \quad (59)$$

where $\deg \tilde{p}^{(i)}(x) < u$. We then write

$$\tilde{b}^{(i)}(x) \tilde{\Lambda}(x) = x^{n^{(i)}-\tau^{(i)}+u} \tilde{q}^{(i)}(x) + \tilde{p}^{(i)}(x) \quad (60)$$

for some (unique) $\tilde{q}^{(i)}(x)$ with $\deg \tilde{q}^{(i)}(x) < \deg \tilde{\Lambda}(x)$.

Further, let

$$\hat{\Lambda}(x) \triangleq x^u \tilde{\Lambda}(x^{-1}) \quad (61)$$

$$\hat{p}^{(i)}(x) \triangleq x^{u-1} \tilde{p}^{(i)}(x^{-1}) \quad (62)$$

$$\hat{q}^{(i)}(x) \triangleq x^{u-1} \tilde{q}^{(i)}(x^{-1}). \quad (63)$$

By substituting x^{-1} for x in (60) and multiplying both sides by $x^{n^{(i)}-\tau^{(i)}+2u-1}$, we obtain

$$s^{(i)}(x)\hat{\Lambda}(x) = x^{n^{(i)}-\tau^{(i)}+u}\hat{p}^{(i)}(x) + \hat{q}^{(i)}(x), \quad (64)$$

where $s^{(i)}(x)$ is obtained from (40). It follows that

$$s^{(i)}(x)\hat{\Lambda}(x) \equiv \hat{q}^{(i)}(x) \pmod{x^{n^{(i)}-\tau^{(i)}+u}} \quad (65)$$

and therefore

$$w^{(i)}(x)\bar{b}^{(i)}(x)\hat{\Lambda}(x) \equiv \hat{q}^{(i)}(x) \pmod{x^{n^{(i)}-\tau^{(i)}+u}}. \quad (66)$$

By multiplying both sides of (66) by $\bar{m}^{(i)}(x)$, we obtain

$$\bar{b}^{(i)}(x)\hat{\Lambda}(x) \equiv \hat{q}^{(i)}(x)\bar{m}^{(i)}(x) \pmod{x^{n^{(i)}-\tau^{(i)}+u}}, \quad (67)$$

and therefore

$$\bar{b}^{(i)}(x)\hat{\Lambda}(x) - \hat{q}^{(i)}(x)\bar{m}^{(i)}(x) = x^{n^{(i)}-\tau^{(i)}+u}\hat{r}^{(i)}(x) \quad (68)$$

holds for some (unique) $\hat{r}^{(i)}(x)$ with $\deg \hat{r}^{(i)}(x) < \tau^{(i)}$. Let

$$\hat{r}^{(i)}(x) \triangleq x^{\tau^{(i)}-1}\hat{r}^{(i)}(x^{-1}). \quad (69)$$

By substituting x^{-1} for x in (68) and multiplying both sides by $x^{n^{(i)}+u-1}$, we obtain

$$b^{(i)}(x)\tilde{\Lambda}(x) - \tilde{q}^{(i)}(x)m^{(i)}(x) = \tilde{r}^{(i)}(x) \quad (70)$$

and therefore

$$\deg(b^{(i)}(x)\tilde{\Lambda}(x) \bmod m^{(i)}(x)) < \tau^{(i)}. \quad (71)$$

Clearly, $\tilde{\Lambda}(x)$ satisfies (1), and (57) follows. \square

IV. SIMULTANEOUS PARTIAL-INVERSE ALGORITHMS

We now consider algorithms to solve the simultaneous partial-inverse problem as stated in Section I. We give both a basic algorithm, which resembles the multi-sequence shift register synthesis algorithm [6], and two variations of it. In the special case where $L = 1$, these algorithms reduce to their counterparts in [4, Section IV].

A. The Basic Algorithm (Algorithm 1)

The basic algorithm is stated as *Algorithm 1* in the framed box: Lines 1–8 are for initialization; the nontrivial part begins with line 9. Note that lines 21–23 simply swap $\Lambda(x)$ with $\Lambda^{(i)}(x)$, d with $d^{(i)}$, and κ with $\kappa^{(i)}$. The only actual computations are in lines 18 and 26. Note that in line 18, we have $\kappa = 0$ if $d \geq \deg m^{(i)}(x)$.

We now begin to explain the algorithm (but the detailed proof of correctness will be given in Section VIII). To this end, we define the following quantities. For any nonzero $\Lambda(x)$ and any $i \in \{1, 2, \dots, L\}$, let

$$\text{rd}^{(i)}(\Lambda) \triangleq \deg(b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x)), \quad (72)$$

$$\delta_{\max}(\Lambda) \triangleq \max_{i \in \{1, \dots, L\}} \left(\text{rd}^{(i)}(\Lambda) - \tau^{(i)} \right), \quad (73)$$

and

$$i_{\max}(\Lambda) \triangleq \max_{i \in \{1, \dots, L\}} \arg\max \left(\text{rd}^{(i)}(\Lambda) - \tau^{(i)} \right), \quad (74)$$

Algorithm 1: Simultaneous Partial-Inverse Algorithm

Input: $b^{(i)}(x), m^{(i)}(x), \tau^{(i)}$ for $i = 1, \dots, L$.

Output: $\Lambda(x)$ as in the problem statement.

```

1  for  $i = 1, \dots, L$  begin
2       $\Lambda^{(i)}(x) := 0$ 
3       $d^{(i)} := \deg m^{(i)}(x)$ 
4       $\kappa^{(i)} := \text{lcf } m^{(i)}(x)$ 
5  end
6   $\Lambda(x) := 1$ 
7   $\delta := \max_{i \in \{1, \dots, L\}} (\deg m^{(i)}(x) - \tau^{(i)})$ 
8   $i := 1$ 
9  loop begin
10     repeat
11         if  $i > 1$  begin  $i := i - 1$  end
12         else begin
13             if  $\delta \leq 0$  return  $\Lambda(x)$ 
14              $i := L$ 
15              $\delta := \delta - 1$ 
16         end
17          $d := \delta + \tau^{(i)}$ 
18          $\kappa := \text{coefficient of } x^d \text{ in}$ 
19              $b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x)$ 
20     until  $\kappa \neq 0$ 
21     if  $d < d^{(i)}$  begin
22         swap  $(\Lambda(x), \Lambda^{(i)}(x))$ 
23         swap  $(d, d^{(i)})$ 
24         swap  $(\kappa, \kappa^{(i)})$ 
25          $\delta := d - \tau^{(i)}$ 
26     end
27      $\Lambda(x) := \kappa^{(i)}\Lambda(x) - \kappa x^{d-d^{(i)}}\Lambda^{(i)}(x)$ 
28 end

```

See also the refinement in Algorithm 1.A below.

Algorithm 1.A: In the special case $m^{(i)}(x) = x^{\deg m^{(i)}}$, line 18 of Algorithm 1 amounts to

$$31 \quad \kappa := b_d^{(i)}\Lambda_0 + b_{d-1}^{(i)}\Lambda_1 + \dots + b_{d-\nu}^{(i)}\Lambda_\nu$$

with $\nu \triangleq \deg \Lambda(x)$ and where $b_\ell^{(i)} \triangleq 0$ for $\ell < 0$.

In another special case where $m^{(i)}(x) = x^{\deg m^{(i)}} - 1$, line 18 becomes

$$51 \quad \kappa := b_d^{(i)}\Lambda_0 + b_{[d-1]}^{(i)}\Lambda_1 + \dots + b_{[d-\nu]}^{(i)}\Lambda_\nu$$

with $b_{[\ell]}^{(i)} \triangleq b_\ell^{(i)} \bmod n$.

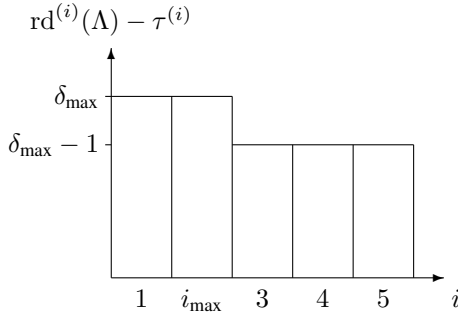


Fig. 1. Illustration of (73) and (74) for $i_{\max} = 2$.

the largest among the indices i that maximize $\text{rd}^{(i)}(\Lambda) - \tau^{(i)}$, cf. Figure 1.

At any given time, the algorithm works on the polynomial $\Lambda(x)$. The inner **repeat** loop (lines 10–19) computes the quantities defined in (72)–(74): between lines 19 and 20, we have

$$i = i_{\max}(\Lambda), \quad \delta = \delta_{\max}(\Lambda), \quad d = \text{rd}^{(i)}(\Lambda), \quad (75)$$

and also

$$\kappa = \text{lcf}(b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x)). \quad (76)$$

In particular, the very first execution of the **repeat** loop (with $\Lambda(x) = 1$) yields

$$i = \max \operatorname{argmax}_{i \in \{1, \dots, L\}} \left(\deg b^{(i)} - \tau^{(i)} \right), \quad (77)$$

$d = \deg b^{(i)}(x)$, and $\kappa = \text{lcf } b^{(i)}(x)$ between lines 19 and 20.

In the special case $L = 1$, lines 11–17 (excluding line 13) amount to $d := d - 1$; in this case, the algorithm reduces to the partial-inverse algorithm of [3], [4].

The only exit from the algorithm is line 13. Since $\delta \geq \delta_{\max}(\Lambda)$, the condition $\delta \leq 0$ guarantees that $\Lambda(x)$ satisfies (1).

The algorithm maintains the auxiliary polynomials $\Lambda^{(i)}(x)$, $i = 1, \dots, L$, which are all initialized to $\Lambda^{(i)}(x) = 0$. Thereafter, however, $\Lambda^{(i)}(x)$ become nonzero (after their first respective execution of lines 21–23) and satisfy

$$i_{\max}(\Lambda^{(i)}) = i. \quad (78)$$

The heart of the algorithm is line 26, which cancels the leading term in

$$b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x) \quad (79)$$

(except for the first execution for each index i , see below). Line 26 is explained by the following lemma.

Lemma 1 (Remainder Decreasing Lemma). Let $\Lambda'(x)$ and $\Lambda''(x)$ be nonzero polynomials such that $i \triangleq i_{\max}(\Lambda') = i_{\max}(\Lambda'')$ and $\text{rd}^{(i)}(\Lambda') \geq \text{rd}^{(i)}(\Lambda'')$. Then $\delta_{\max}(\Lambda') \geq \delta_{\max}(\Lambda'')$ and the polynomial

$$\Lambda(x) \triangleq \kappa'' \Lambda'(x) - \kappa' x^{d' - d''} \Lambda''(x) \quad (80)$$

with $d' \triangleq \text{rd}^{(i)}(\Lambda')$, $\kappa' \triangleq \text{lcf}(b^{(i)}(x)\Lambda'(x) \bmod m^{(i)}(x))$, $d'' \triangleq \text{rd}^{(i)}(\Lambda'')$, and $\kappa'' \triangleq \text{lcf}(b^{(i)}(x)\Lambda''(x) \bmod m^{(i)}(x))$ satisfies both

$$\text{rd}^{(i)}(\Lambda) < \text{rd}^{(i)}(\Lambda') \quad (81)$$

and

$$\delta_{\max}(\Lambda) \leq \delta_{\max}(\Lambda') \quad (82)$$

and either

$$i_{\max}(\Lambda) < i_{\max}(\Lambda'), \quad (83)$$

or

$$\delta_{\max}(\Lambda) < \delta_{\max}(\Lambda'). \quad (84)$$

□

The lemma is proved in Section VIII-A. It follows from (81)–(84) that the algorithm makes progress and eventually terminates.

For each index $i \in \{1, \dots, L\}$, when line 26 is executed for the very first time, it is necessarily preceded by the swap in lines 21–23. In this case, line 26 reduces to

$$\Lambda(x) := -\left(\text{lcf } m^{(i)}(x)\right) x^{\deg m^{(i)}(x) - \text{rd}^{(i)}(\Lambda')} \Lambda'(x) \quad (85)$$

where $\Lambda'(x)$ is the value of $\Lambda(x)$ before the swap. It follows, in particular, that $\deg \Lambda(x) > \deg \Lambda'(x)$.

In any case, we always have

$$\deg(b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x)) < d \quad (86)$$

after executing line 26.

Finally, we note that every execution of the swap in lines 21–23 strictly reduces $d^{(i)}$. We also note that the execution of line 24 results in

$$\delta = \begin{cases} \delta_{\max}(\Lambda), & \text{if } \Lambda(x) \neq 0 \\ \deg m^{(i)} - \tau^{(i)}, & \text{if } \Lambda(x) = 0, \end{cases} \quad (87)$$

where the second case happens only once—the very first time—for each index $i \in \{1, \dots, L\}$.

Theorem 2 (Simultaneous Partial-Inverse Algorithm). Algorithm 1 returns the solution of the simultaneous partial-inverse problem. □

The proof will be given in Section VIII.

B. Complexity of Algorithm 1

Let

$$B \triangleq L \max_{i \in \{1, \dots, L\}} (\deg m^{(i)}(x) - \tau^{(i)}). \quad (88)$$

and note that D as in (21) satisfies $D \leq B$. The complexity of the basic SPI algorithm is determined by

Theorem 3 (Complexity). The number N_{it} of executions of line 18 is bounded by $N_{\text{it}} \leq (L + 1)B$. □

Proof: We associate the polynomials $\Lambda(x)$ and $\Lambda^{(i)}(x)$ with the additional variables n_{it} and $n_{\text{it}}^{(i)}$. These variables are initialized to zero and swapped whenever $\Lambda(x)$ and $\Lambda^{(i)}(x)$ are swapped. Moreover, n_{it} is incremented in every execution of line 18. When the algorithm stops, we have $N_{\text{it}} = n_{\text{it}} + \sum_{i=1}^L n_{\text{it}}^{(i)}$. The theorem then follows from $n_{\text{it}} \leq B$ and $n_{\text{it}}^{(i)} \leq n_{\text{it}}$. ■

In the special case $L = 1$, the theorem reduces to [4, (94) of Theorem 5].

Now, let

$$h \triangleq \max_{i \in \{1, \dots, L\}} (\deg m^{(i)}(x)) \quad (89)$$

and let

$$g \triangleq \min(h, \deg \Lambda(x)) \quad (90)$$

where $\Lambda(x)$ is the solution of the SPI problem.

In the special cases where $m^{(i)}(x) = x^{\deg m^{(i)}(x)}$ and/or $m^{(i)}(x) = x^{\deg m^{(i)}(x)} - 1$ for all $i \in \{1, \dots, L\}$, The complexity of Algorithm 1 (with Algorithm 1.A) is $O(LBg)$ by Theorem 3; in these cases, the algorithm looks like, and is as efficient as, the generalized Berlekamp-Massey algorithm [6] (see also [19]).

For a SPI problem with general $m^{(i)}(x)$, the same complexity can be achieved by first transforming the original SPI problem into a monomialized SPI problem as in Theorem 1, and then solving the transformed problem.

Alternatively, the SPI problem with general $m^{(i)}(x)$ can be solved by two easy variations of Algorithm 1 below, which, however, have higher complexity than with Algorithm 1.A.

C. Quotient Saving Algorithm

Algorithm 2 is a variation of Algorithm 1 that achieves a generalization of Algorithm 1.A to general $m^{(i)}(x)$: line 18 of Algorithm 1 is now line 23 of Algorithm 2.

To this end, we store and update also the quotients $Q^{(i)}(x)$, $i = 1, \dots, L$, defined by

$$b^{(i)}(x)\Lambda(x) = Q^{(i)}(x)m^{(i)}(x) + r^{(i)}(x) \quad (91)$$

with $r^{(i)}(x) \triangleq b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x)$. The coefficient of x^d of $r^{(i)}(x)$ in line 18 of Algorithm 1 can then be computed as

$$\kappa := \sum_{\ell=0}^u b_{d-\ell}^{(i)} \Lambda_{\ell} - \sum_{\ell=0}^v m_{d-\ell}^{(i)} Q_{\ell}^{(i)} \quad (92)$$

with $u \triangleq \deg \Lambda(x)$ and $v \triangleq \deg Q^{(i)}(x)$, and where $b_{\ell}^{(i)} \triangleq 0$ for both $\ell < 0$ and $\ell > \deg b^{(i)}(x)$, and where $m_{\ell}^{(i)} \triangleq 0$ for both $\ell < 0$ and $\ell > \deg m^{(i)}(x)$.

The quotients $Q^{(i)}(x)$ of (91) are initialized in line 11 and updated in line 34 in the same fashion as $\Lambda(x)$. Following $\Lambda(x)$, these quotients $Q^{(i)}(x)$ are stored in line 29, where $Q^{(i,j)}(x)$ are initialized in lines 5–8.

All other quantities in the algorithm remain unchanged. Algorithm 2 works exactly the same as Algorithm 1. In any case (as in (86)), we always have

$$\deg(b^{(i)}(x)\Lambda(x) - Q^{(i)}(x)m^{(i)}(x)) < d \quad (93)$$

after executing lines 33–35.

Due to the additional computation of lines 33–35, the complexity of Algorithm 2 is $O(L^2Bg)$ with g in (90).

D. Remainder Saving Algorithm

Another variation of Algorithm 1 is Algorithm 3, where we instead store and update the remainders $r^{(i)}(x)$ of (91) for $i = 1, \dots, L$. In consequence, the computation of line 18 of Algorithm 1 (which is now line 23 of Algorithm 3) is unnecessary; however, the additional computation in lines 33–35 is required.

Algorithm 2: Quotient Saving SPI Algorithm

Input: $b^{(i)}(x), m^{(i)}(x), \tau^{(i)}$ for $i = 1, \dots, L$.

Output: $\Lambda(x)$ as in the problem statement.

```

1  for  $i = 1, \dots, L$  begin
2     $\Lambda^{(i)}(x) := 0$ 
3     $d^{(i)} := \deg m^{(i)}(x)$ 
4     $\kappa^{(i)} := \text{lcf } m^{(i)}(x)$ 
5    for  $j = 1, \dots, L$  begin
6       $Q^{(i,j)}(x) := 0$ 
7      if  $i = j$  begin  $Q^{(i,j)}(x) := -1$  end
8    end
9  end
10  $\Lambda(x) := 1$ 
11 for  $i = 1, \dots, L$  begin  $Q^{(i)}(x) := 0$  end
12  $\delta := \max_{i \in \{1, \dots, L\}} (\deg m^{(i)}(x) - \tau^{(i)})$ 
13  $i := 1$ 
14 loop begin
15   repeat
16     if  $i > 1$  begin  $i := i - 1$  end
17     else begin
18       if  $\delta \leq 0$  return  $\Lambda(x)$ 
19        $i := L$ 
20        $\delta := \delta - 1$ 
21     end
22      $d := \delta + \tau^{(i)}$ 
23      $\kappa := \sum_{\ell=0}^u b_{d-\ell}^{(i)} \Lambda_{\ell} - \sum_{\ell=0}^v m_{d-\ell}^{(i)} Q_{\ell}^{(i)}$ 
24   until  $\kappa \neq 0$ 
25   if  $d < d^{(i)}$  begin
26     swap ( $\Lambda(x), \Lambda^{(i)}(x)$ )
27     swap ( $d, d^{(i)}$ )
28     swap ( $\kappa, \kappa^{(i)}$ )
29     for  $j = 1, \dots, L$  swap ( $Q^{(j)}(x), Q^{(i,j)}(x)$ )
30      $\delta := d - \tau^{(i)}$ 
31   end
32    $\Lambda(x) := \kappa^{(i)} \Lambda(x) - \kappa x^{d-d^{(i)}} \Lambda^{(i)}(x)$ 
33   for  $j = 1, \dots, L$  begin
34      $Q^{(j)}(x) := \kappa^{(i)} Q^{(j)}(x) - \kappa x^{d-d^{(i)}} Q^{(i,j)}(x)$ 
35   end
36 end

```

With the corresponding replacements of $Q^{(i)}(x)$ and $Q^{(i,j)}(x)$ by $r^{(i)}(x)$ and $r^{(i,j)}(x)$, Algorithm 3 works exactly the same as Algorithms 1 and 2. In any case, we have

$$\deg r^{(i)}(x) < d \quad (94)$$

after executing lines 33–35.

Due to the additional computation of lines 33–35, the complexity of Algorithm 3 is $O(L^2Bh)$ with h in (89).

V. ABOUT INTERLEAVED REED-SOLOMON CODES

Decoding interleaved Reed-Solomon codes beyond half the minimum distance can be reduced rather naturally to the

Algorithm 3: Remainder Saving SPI AlgorithmInput: $b^{(i)}(x), m^{(i)}(x), \tau^{(i)}$ for $i = 1, \dots, L$.Output: $\Lambda(x)$ as in the problem statement.

```

1  for  $i = 1, \dots, L$  begin
2     $\Lambda^{(i)}(x) := 0$ 
3     $d^{(i)} := \deg m^{(i)}(x)$ 
4     $\kappa^{(i)} := \text{lcf } m^{(i)}(x)$ 
5    for  $j = 1, \dots, L$  begin
6       $r^{(i,j)}(x) := 0$ 
7      if  $i = j$  begin  $r^{(i,j)}(x) := m^{(i)}(x)$  end
8    end
9  end
10  $\Lambda(x) := 1$ 
11 for  $i = 1, \dots, L$  begin  $r^{(i)}(x) := b^{(i)}(x)$  end
12  $\delta := \max_{i \in \{1, \dots, L\}} (\deg m^{(i)}(x) - \tau^{(i)})$ 
13  $i := 1$ 
14 loop begin
15   repeat
16     if  $i > 1$  begin  $i := i - 1$  end
17     else begin
18       if  $\delta \leq 0$  return  $\Lambda(x)$ 
19        $i := L$ 
20        $\delta := \delta - 1$ 
21     end
22      $d := \delta + \tau^{(i)}$ 
23      $\kappa := \text{coefficient of } x^d \text{ of } r^{(i)}(x)$ 
24   until  $\kappa \neq 0$ 
25   if  $d < d^{(i)}$  begin
26     swap  $(\Lambda(x), \Lambda^{(i)}(x))$ 
27     swap  $(d, d^{(i)})$ 
28     swap  $(\kappa, \kappa^{(i)})$ 
29     for  $j = 1, \dots, L$  swap  $(r^{(j)}(x), r^{(i,j)}(x))$ 
30      $\delta := d - \tau^{(i)}$ 
31   end
32    $\Lambda(x) := \kappa^{(i)} \Lambda(x) - \kappa x^{d-d^{(i)}} \Lambda^{(i)}(x)$ 
33   for  $j = 1, \dots, L$  begin
34      $r^{(j)}(x) := \kappa^{(i)} r^{(j)}(x) - \kappa x^{d-d^{(i)}} r^{(i,j)}(x)$ 
35   end
36 end

```

simultaneous partial inverse problem of Section I. We begin with the following (more or less standard) concepts (see also [4]); the actual decoding algorithms will be given in Section VI.

A. Array Codes and Evaluation Isomorphism

Let $F = F_q$ be a finite field with q elements, and consider array codes as stated in Section I where codewords are $L \times n$ arrays over F such that each row is a codeword in the same (n, k) Reed-Solomon code (3). As noted in [8], [12], [13], such interleaved Reed-Solomon codes can be equivalently viewed as shortened Reed-Solomon codes (sub-field evaluation codes)

over F_{q^L} . (The generalization to the cases where row codes have different k will be addressed in Appendix A.)

Let

$$m(x) \triangleq \prod_{\ell=0}^{n-1} (x - \beta_\ell), \quad (95)$$

where $\deg m(x) = n$. Let ψ be the evaluation mapping

$$\psi : F[x]/m(x) \rightarrow F^n : a(x) \mapsto (a(\beta_0), \dots, a(\beta_{n-1})), \quad (96)$$

which is a ring isomorphism. The row code (3) can then be described as

$$\{c \in F^n : \deg \psi^{-1}(c) < k\}. \quad (97)$$

The standard definition of Reed-Solomon codes requires, in addition, that

$$\beta_\ell = \alpha^\ell \text{ for } \ell = 0, \dots, n-1, \quad (98)$$

where $\alpha \in F$ is a primitive n -th root of unity. This addition condition implies

$$m(x) = x^n - 1, \quad (99)$$

and turns ψ into a discrete Fourier transform [21]. However, (98) and (99) will not be required below. In particular, the set $\{\beta_0, \dots, \beta_{n-1}\}$ will be permitted to contain 0.

In general, the inverse mapping ψ^{-1} may be computed by Lagrange interpolation or according to the Chinese remainder theorem. (For the latter, see also [22], [23].)

B. Notation for Individual Rows and Error Support

Let $Y = C + E \in F^{L \times n}$ be the received word where $C \in F^{L \times n}$ is the transmitted (array-) codeword and $E \in F^{L \times n}$ is the error pattern. Further, let $y^{(i)}$ be the i -th row of the matrix Y , let $c^{(i)}$ be the i -th row of C , and let $e^{(i)}$ be the i -th row of E . We then have $y^{(i)} = c^{(i)} + e^{(i)}$, $i = 1, \dots, L$, and therefore

$$Y^{(i)}(x) = a^{(i)}(x) + E^{(i)}(x) \quad (100)$$

where $Y^{(i)}(x) \triangleq \psi^{-1}(y^{(i)})$, $a^{(i)}(x) \triangleq \psi^{-1}(c^{(i)})$, and $E^{(i)}(x) \triangleq \psi^{-1}(e^{(i)})$. Note that $\deg E^{(i)}(x) < \deg m(x) = n$ and $\deg a^{(i)}(x) < k$.

We will index the columns of codewords and error patterns beginning with zero as in $E = (e_0, \dots, e_{n-1})$, and we denote by $U_E \subset \{0, \dots, n-1\}$ the index set of the nonzero columns of E , i.e.,

$$U_E \triangleq \{\ell \in \{0, \dots, n-1\} : e_\ell \neq 0\}. \quad (101)$$

We will only consider column errors, and will not distinguish between columns with a single error and columns with many errors. Note that symbol errors in F_{q^L} correspond to column errors in the array code.

The error-locator polynomial is then defined as

$$\Lambda_E(x) \triangleq \prod_{j \in U_E} (x - \beta_j). \quad (102)$$

Note that

$$|U_E| = \deg \Lambda_E(x) = \text{number of column errors}, \quad (103)$$

and we assume below $|U_E| \leq n - k$.

C. Error Locator Polynomial and Interpolation

If an estimate of the error locator polynomial $\Lambda(x) = \gamma\Lambda_E(x)$ (with nonzero $\gamma \in F$) is known, the polynomial $a^{(i)}(x)$ for each $i \in \{1, \dots, L\}$ can be recovered in many different ways (as discussed in [4]), e.g., by means of

$$a^{(i)}(x) = \frac{Y^{(i)}(x)\Lambda(x) \bmod m(x)}{\Lambda(x)} \quad (104)$$

according to [4, Proposition 8](see also [22], [23]), or by means of

$$a^{(i)}(x) = Y^{(i)}(x) \bmod \tilde{m}(x) \quad (105)$$

with $\tilde{m}(x) \triangleq m(x)/\Lambda(x)$ according to [4, Proposition 9]. In the special case where $m(x) = x^n - 1$, computing the numerator in (104) amounts to a cyclic convolution. If L is large, recovery via (105) appears to be more attractive.

If we need to recover the actual codeword $c^{(i)}$ (rather than just the polynomial $a^{(i)}(x)$), interpolation according to (104) or (105) requires the additional computation of $\psi(a^{(i)}(x))$. Alternatively, it may be attractive to compute the error pattern $e^{(i)} = y^{(i)} - c^{(i)}$ by [4, Propositions 10 and 11]: for nonzero polynomial $\Lambda(x) = \gamma\Lambda_E(x)$, let

$$Q^{(i)}(x) \triangleq Y^{(i)}(x)\Lambda(x) \bmod m(x); \quad (106)$$

then by Forney's formula

$$e_\ell^{(i)} \triangleq \begin{cases} 0 & \text{if } \Lambda(\beta_\ell) \neq 0 \\ \frac{Q^{(i)}(\beta_\ell)m'(\beta_\ell)}{\Lambda'(\beta_\ell)} & \text{if } \Lambda(\beta_\ell) = 0 \end{cases} \quad (107)$$

for $\ell = 0, 1, \dots, n-1$, where $\Lambda'(x)$ and $m'(x)$ denote the formal derivatives of $\Lambda(x)$ and $m(x)$, respectively.

VI. DECODING VIA SIMULTANEOUS PARTIAL INVERSES

We now present efficient algorithms for decoding the array codes of Section V. The heart of these algorithms is a method for computing (an estimate of) the error locator polynomial $\Lambda_E(x)$, which amounts to solving a simultaneous partial-inverse problem.

A. The SPI Error-Locating Equation

The definition of (102) implies

$$E^{(i)}(x)\Lambda_E(x) \bmod m(x) = 0, \quad (108)$$

and therefore

$$\deg(Y^{(i)}(x)\Lambda_E(x) \bmod m(x)) < k + |U_E| \quad (109)$$

hold for all $i \in \{1, \dots, L\}$.

Lemma 2 (The SPI Problem). Consider a SPI problem as in Section I with $b^{(i)}(x) = Y^{(i)}(x)$, $m^{(i)}(x) = m(x)$, and $\tau^{(i)} = k + |U_E|$ for $i = 1, \dots, L$; then its solution $\Lambda(x)$ satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k + |U_E| \quad (110)$$

with $\deg \Lambda(x) \leq |U_E|$. \square

Proof: It is immediate from Proposition 1 and (109). \blacksquare

Lemma 3 (SPI Error-Locating Equation). If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (110), then $\Lambda(x)$ is a nonzero polynomial (unique up to a scale factor) of the smallest degree that satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k + \deg \Lambda(x) \quad (111)$$

simultaneously for all $i \in \{1, \dots, L\}$. \square

Proof: Obviously, the solution $\Lambda_E(x)$ of the SPI problem (110) satisfies (111). If some nonzero $\Lambda(x)$ with $\deg \Lambda(x) < |U_E|$ satisfies (111), then $\Lambda(x)$ also satisfy (110), which leads to a contradiction. Uniqueness follows from that any SPI problem has a unique solution, cf. Proposition 2. \blacksquare

B. The SPI Error-Locating Algorithm

Lemmas 2 and 3 suggest the following algorithm to find the error locator polynomial $\Lambda_E(x)$.

The SPI Error-Locating Algorithm:

- 1) Run any of the SPI algorithms of Section IV with $b^{(i)}(x) = Y^{(i)}(x)$ in (100), $m^{(i)}(x) = m(x)$ in (95), and $\tau^{(i)} = \deg m^{(i)}(x) - 1$ for $i \in \{1, \dots, L\}$.
- 2) If the returned polynomial $\Lambda(x)$ satisfies the condition

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k + \deg \Lambda(x) \quad (112)$$

for every $i \in \{1, \dots, L\}$, then stop.

- 3) Otherwise, decrease all $\tau^{(i)}$ by 1 and continue the SPI algorithm.
- 4) Go to 2). \square

The test (112) requires no extra computations. Indeed, this error locating method can be implemented by modifying Algorithm 1 of Section IV as Algorithm 4 (see box) with

$$b^{(i)}(x) = Y^{(i)}(x), \quad m^{(i)}(x) = m(x), \quad \tau^{(i)} = n - 1, \quad (113)$$

and (the additional input) $\bar{k}^{(i)} = k$. Note that line 72 suffices to check (112) for all i , and we have $\tau^{(1)} = \dots = \tau^{(L)}$ throughout the algorithm. Alternatively, the error locating method can be implemented as Algorithm 5 and/or Algorithm 6.

Theorem 4. If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (110), then each of Algorithms 4–6 with (113) and $\bar{k}^{(i)} = k$ stops with $\tau^{(i)} \geq k + |U_E|$ and returns $\Lambda(x) = \gamma\Lambda_E(x)$ for some nonzero $\gamma \in F$. \square

Proof: It is immediate from Lemmas 2 and 3, and assume that the underlying SPI algorithm is correct. (Correctness of the basic SPI algorithm is proved in Section VIII.) \blacksquare

In the following two subsections, we investigate the error-locating capability of Algorithms 4–6; the actual decoding algorithm will be given in Section VI-H below.

C. Guaranteed Error-Locating Capability

The justification of Algorithms 4–6 hinges on the theorem.

Theorem 5 (Sufficient Condition). Let r_E be the rank of the submatrix formed by nonzero columns of E . If

$$2|U_E| < n - k + r_E \quad (114)$$

Algorithm 4: SPI Error-Locating AlgorithmInput: $b^{(i)}(x), m^{(i)}(x), \tau^{(i)}, \bar{k}^{(i)}$ for $i = 1, \dots, L$.Output: nonzero $\Lambda(x) \in F[x]$, a candidate for the error locator $\Lambda_E(x)$ (up to a scale factor).

The algorithm is the same as Algorithm 1 of Section IV except that its line 13 is replaced by following lines:

```

71  if  $\delta \leq 0$  begin
72      if  $d \leq \deg \Lambda(x) + \bar{k}^{(i)}$  return  $\Lambda(x)$ 
73      else begin
74           $\delta := \delta + 1$ 
75          for  $j = 1, \dots, L$  begin  $\tau^{(j)} := \tau^{(j)} - 1$  end
76      end
77  end

```

Algorithm 5: QS-SPI Error-Locating AlgorithmInput: $b^{(i)}(x), m^{(i)}(x), \tau^{(i)}, \bar{k}^{(i)}$ for $i = 1, \dots, L$ Output: nonzero $\Lambda(x) \in F[x]$, a candidate for the error locator $\Lambda_E(x)$ (up to a scale factor).

The algorithm is the same as Algorithm 2 of Section IV except that its line 18 is replaced by lines 71–77 as in Algorithm 4.

Algorithm 6: RS-SPI Error-Locating AlgorithmInput: $b^{(i)}(x), m^{(i)}(x), \tau^{(i)}, \bar{k}^{(i)}$ for $i = 1, \dots, L$ Output: nonzero $\Lambda(x) \in F[x]$, a candidate for the error locator $\Lambda_E(x)$ (up to a scale factor).

The algorithm is the same as Algorithm 3 of Section IV except that its line 18 is replaced by lines 71–77 as in Algorithm 4.

then $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (110). \square

The proof will be given in Section VII. (For the proof, Theorem 9 is essential.)

By Theorems 4 and 5, Algorithms 4–6 (with (113) and $\bar{k}^{(i)} = k$) are guaranteed to return $\Lambda(x) = \gamma \Lambda_E(x)$ if

$$|U_E| \leq \frac{n - k + r_E - 1}{2} \quad (115)$$

which agrees with the guarantee in [10], and which improves on Theorem 2 of [8] by a margin of $r_E/2$.It is instructive to consider the special case $r_E = |U_E|$, which is very likely if $|U_E| \leq L$, cf. Proposition 7 below. In this case, (114) reduces to

$$|U_E| < n - k, \quad (116)$$

and we have the following improvement on Theorem 4.

Proposition 6 (Full-Rank-Error Location). If

$$r_E = |U_E| < n - k, \quad (117)$$

then the SPI error-locating algorithm of Section VI-B stops with $\tau^{(i)} = \deg m^{(i)}(x) - 1$ (i.e., when (112) is checked for the very first time) and returns $\Lambda(x) = \gamma \Lambda_E(x)$ for some nonzero $\gamma \in F$. \square The proof will be given in Section VII. Recall that $q \triangleq |F|$.**Proposition 7 (Full-Rank Probability).** If $|U_E| \leq L$ and if the $|U_E|$ nonzero columns of the $L \times n$ matrix E are uniformly and independently distributed over $F^L \setminus \{0\}$, then

$$\Pr(r_E \neq |U_E|) < \frac{q^{-L+|U_E|}}{q-1} \quad (118)$$

 \square

The proof is given in Section VII.

Propositions 6 and 7 show, in particular, that the SPI error-locating algorithm can be very efficient even if L is large.**D. Statistical Error-Locating Capability**We now consider random errors without the constraint $|U_E| \leq L$.**Lemma 4.** Assume $L > 1$. If the $|U_E|$ nonzero columns of E are uniformly distributed over $F_q^L \setminus \{0\}$, then the probability P_Λ that $\Lambda_E(x)$ does not solve the SPI problem (110) is bounded by

$$P_\Lambda < \frac{q^{-L(n-k)+(L+1)|U_E|}}{q-1} \quad (119)$$

 \square

The proof is given in Section VII.

Theorem 6. Assume $L > 1$. If E has distribution as in Lemma 4, then the probability P_f that the SPI error-locating algorithm of Section VI-B fails to find $\Lambda(x) = \gamma \Lambda_E(x)$ is bounded by

$$P_f < \frac{q^{-L(n-k)+(L+1)|U_E|}}{q-1} \quad (120)$$

 \square *Proof:* The theorem follows from Theorem 4, Lemma 4, and the fact that $P_f \leq P_\Lambda$. \blacksquare For $|U_E| \leq L$, both (118) and (120) apply. In general, the bound (118) is much weaker than (120), but the bounds agree in the special case where $|U_E| = n - k - 1$; in this special case, these bounds agree also with the bounds in [10], [16], [18] (where different decoding algorithms are used).Note that (120) implies that the SPI error-locating algorithm can correctly locate errors (with high probability, if q is large) up to the radius

$$|U_E| \leq \frac{L}{L+1}(n-k). \quad (121)$$

The bound (120) improves (almost agrees with, but is strictly better than) the best prior bound of [8], and it beats the bound of [7].

E. A Remark on the SPI Problem (110)In contrast to (114), the bound (121) is a *necessary* condition for $\Lambda_E(x)$ to solve the SPI problem (110): by Proposition 3, if $\Lambda_E(x)$ solves the SPI problem (110), then

$$|U_E| \leq L(n-k-|U_E|), \quad (122)$$

which coincides with (121).

F. The Reduced SPI Error-Locating Equation

If $\Lambda_E(x)$ solves the SPI problem (110), then from (22), coefficients $Y_\ell^{(i)}$ of $Y^{(i)}(x)$ for

$$\begin{aligned} \ell &< k + |U_E| - L(n - k - |U_E|) \\ &\leq k \end{aligned}$$

(where the last step is easily seen from (122)) are irrelevant and can be set to zero.

Lemma 5 (Reduced SPI Problem). Let

$$\tilde{Y}^{(i)}(x) \triangleq Y_k^{(i)} + Y_{k+1}^{(i)}x + \dots + Y_{n-1}^{(i)}x^{n-k-1} \quad (123)$$

for $i = 1, \dots, L$, and let

$$\tilde{m}(x) \triangleq m_k + m_{k+1}x + \dots + m_n x^{n-k}. \quad (124)$$

Then $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (110) if and only if it solves the SPI problem

$$\deg(\tilde{Y}^{(i)}(x)\Lambda(x) \bmod \tilde{m}(x)) < |U_E|. \quad (125)$$

Proof: It follows from Proposition 5 with $s^{(i)} = k$. ■

We then have the following counterpart of Lemma 3.

Lemma 6 (Reduced SPI Error-Locating Equation). If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (125), then $\Lambda(x)$ is a nonzero polynomial of the smallest degree (unique up to a scale factor) that satisfies

$$\deg(\tilde{Y}^{(i)}(x)\Lambda(x) \bmod \tilde{m}(x)) < \deg \Lambda(x) \quad (126)$$

simultaneously for all $i \in \{1, \dots, L\}$. □

The proof follows from an obvious adaption of the proof of Lemma 3: replacing (110) by (125) and (111) by (126).

Note that $\deg \tilde{m}(x) = n - k$. Then by Lemmas 5 and 6, the error-locating algorithm of Section VI-B become as follows.

The Reduced SPI Error-Locating Algorithm:

- 1) Run any of the SPI algorithms of Section IV with $b^{(i)}(x) = \tilde{Y}^{(i)}(x)$ in (123), $m^{(i)}(x) = \tilde{m}(x)$ in (124), and $\tau^{(i)} = \deg m^{(i)}(x) - 1$ for $i \in \{1, \dots, L\}$.
- 2) If the returned polynomial $\Lambda(x)$ satisfies the condition

$$\deg(\tilde{Y}^{(i)}(x)\Lambda(x) \bmod \tilde{m}(x)) < \deg \Lambda(x) \quad (127)$$

for every $i \in \{1, \dots, L\}$, then stop.

- 3) Otherwise, decrease all $\tau^{(i)}$ by 1 and continue the SPI algorithm.
- 4) Go to 2). □

This error-locating algorithm can be implemented by any of Algorithms 4–6 with

$$b^{(i)}(x) = \tilde{Y}^{(i)}(x), \quad m^{(i)}(x) = \tilde{m}(x), \quad \tau^{(i)} = n - k - 1, \quad (128)$$

and $\bar{k}^{(i)} = 0$, and we have the counterpart of Theorem 4.

Theorem 7. If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (125), then each of Algorithms 4–6 with (128) and $\bar{k}^{(i)} = 0$ stops with $\tau^{(i)} \geq |U_E|$ and returns $\Lambda(x) = \gamma \Lambda_E(x)$ for some nonzero $\gamma \in F$. □

The proof is an obvious adaption of the proof of Theorem 4.

Note that the error-locating capabilities investigated in Sections VI-C and VI-D hold here, due to the equivalence of the two SPI problems (110) and (125).

G. Monomialized SPI Error-Locating Equation

The SPI problem (110) for general $m(x)$ can be transformed into another SPI problem as follows.

Lemma 7 (Monomialized SPI Problem). For $b^{(i)}(x) = Y^{(i)}(x)$ and $m^{(i)}(x) = m(x)$, let $\tilde{b}^{(i)}(x)$ be the polynomial (40) with $n^{(i)} \triangleq n$, $\tau^{(i)} = k + |U_E|$, and $u \triangleq |U_E|$ for $i = 1, \dots, L$. Then $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (110) if and only if it solves the SPI problem

$$\deg(\tilde{b}^{(i)}(x)\Lambda(x) \bmod x^{n-k}) < |U_E|. \quad (129)$$

□

Proof: It is immediate from Theorem 1. ■

We then have the following counterpart of Lemma 3.

Lemma 8 (Monomialized SPI Error-Locating Equation). If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (129), then $\Lambda(x)$ is a nonzero polynomial of the smallest degree (unique up to a scale factor) that satisfies

$$\deg(\tilde{b}^{(i)}(x)\Lambda(x) \bmod x^{n-k}) < \deg \Lambda(x) \quad (130)$$

simultaneously for all $i \in \{1, \dots, L\}$. □

The proof is an obvious adaption of the proof of Lemma 6.

By Lemmas 5 and 7, the two SPI problems (125) and (129) are equivalent; note also the correspondence between (126) and (130). Clearly, the reduced SPI error-locating algorithm (of Section VI-F) can alternatively be carried out with

$$b^{(i)}(x) = \tilde{b}^{(i)}(x), \quad m^{(i)}(x) = x^{n-k}, \quad \tau^{(i)} = n - k - 1, \quad (131)$$

and we have

Theorem 8. If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (129), then each of Algorithms 4–6 with (131) and $\bar{k}^{(i)} = 0$ stops with $\tau^{(i)} \geq |U_E|$ and returns $\Lambda(x) = \gamma \Lambda_E(x)$ for some nonzero $\gamma \in F$. □

The proof is an obvious adaption of the proof of Theorem 4.

H. The Decoding Algorithms

By Theorems 4, 7, and 8, we thus arrive at the following general decoding procedure:

- 1) Compute $Y^{(i)}(x) = \psi^{-1}(y^{(i)})$ for all i .
- 2) Run any of Algorithms 4–6 with $\bar{k}^{(i)} = k$ and (113), or alternatively with $\bar{k}^{(i)} = 0$ and (128) or (131). If (114) is satisfied, then the polynomial $\Lambda(x)$ returned by the algorithm equals $\Lambda_E(x)$, up to a scale factor.
- 3) Complete decoding, e.g., by means of (104), (105), or by (107), or by other means as described below.

Obviously, this general procedure encompasses a variety of specific algorithms, some of which will be discussed below.

Due to the equivalence of the three SPI problems (110), (125) and (129), the error-locating capabilities investigated in

Sections VI-C and VI-D hold for any of the specific choices of the algorithms in Step 2.

The resulting algorithms are very efficient and guaranteed to correct $|U_E|$ errors up to the radius (114); if $r_E = |U_E|$, (114) reduces to $|U_E| < n - k$, which is very likely if $L \geq |U_E|$. For random errors, they can correct up to the radius (121) with high probability, if q is large.

In addition, there are many opportunities for detecting decoding failure, i.e., checking whether $\Lambda(x) = \gamma \Lambda_E(x)$. A standard method is to check whether $\deg \Lambda(x)$ equals the number of its roots; this check is essential if Forney's formula (107) is used for interpolation; if not satisfied otherwise, then a decoding failure should be declared.

If (104) is used for interpolation, then it should be checked whether $\Lambda(x)$ divides $Y^{(i)}(x)\Lambda(x) \bmod m(x)$; if (105) is used, it should be checked whether $\Lambda(x)$ divides $m(x)$; in the end, the condition $\deg a^{(i)}(x) < k$ should be checked.

We now briefly discuss (as in [4]) some specific choices in Steps 2 and 3 as follows.

1) *Generalized Shiozaki–Gao Decoding*: If Algorithm 6 with $\bar{k}^{(i)} = k$ and (113) is used in Step 2, then Step 3 is naturally carried out via

$$a^{(i)}(x) = r^{(i)}(x)/\Lambda(x), \quad (132)$$

which is immediately from $r^{(i)}(x) = Y^{(i)}(x)\Lambda(x) \bmod m(x)$ and (104). In the special case where $L = 1$, the algorithm reduces to the *Shiozaki–Gao Decoding* discussed in [4].

2) *Generalized Reverse Berlekamp–Massey Decoding*: For $m(x) = x^n - 1$, we use Algorithm 4 (with the refinement in line 31) with $\bar{k}^{(i)} = k$ and (113), or with $\bar{k}^{(i)} = 0$ and (128). Two natural methods for Step 3 are as follows. The first method is to compute the numerator in (104) by

$$r_\ell^{(i)} = \sum_{j=0}^{\tau} Y_{[\ell-j]}^{(i)} \Lambda_j \quad (133)$$

with $\tau \triangleq \deg \Lambda(x)$. Noting that $E_\ell^{(i)} = Y_\ell^{(i)}$ for $\ell \geq k$, a second method (due to (108)) is to compute $E_{k-1}^{(i)}, \dots, E_0^{(i)}$ by the recursion

$$E_{\ell-\tau}^{(i)} = -\frac{1}{\Lambda_\tau} \sum_{j=0}^{\tau-1} E_{\ell-j}^{(i)} \Lambda_j \quad (134)$$

for $\ell = k + \tau - 1, k + \tau - 2, \dots, \tau$. We then obtain $a^{(i)}(x) = Y^{(i)}(x) - E^{(i)}(x)$.

For general $m(x)$, we may use Algorithm 5 with $\bar{k}^{(i)} = k$ and (113), and ask the algorithm to return also $Q^{(i)}(x)$, which satisfy (106). Then, the numerator $r^{(i)}(x)$ in (104) is obtained from $r^{(i)}(x) = Y^{(i)}(x)\Lambda(x) - Q^{(i)}(x)m(x)$. A second method (due to (106)) is to compute $E_{k-1}^{(i)}, \dots, E_0^{(i)}$ from

$$E_{\ell-\tau}^{(i)} = -\frac{1}{\Lambda_\tau} \left(\sum_{j=0}^{\tau-1} E_{\ell-j}^{(i)} \Lambda_j - \sum_{j=0}^{\nu} m_{\ell-j} Q_j^{(i)} \right) \quad (135)$$

for $\ell = k + \tau - 1, k + \tau - 2, \dots, \tau$, where $\nu \triangleq \deg Q^{(i)}(x)$.

For general $m(x)$, using Algorithm 4 with $\bar{k}^{(i)} = 0$ and (131) is a nice alternative; the polynomials $Q^{(i)}(x)$ for all i

can then be obtained from

$$Q^{(i)}(x) = \tilde{b}^{(i)}(x)\Lambda(x) \bmod x^{n-k} \quad (136)$$

according to Theorem 1 and Lemma 7.

If we wish to recover not $a^{(i)}(x)$, but the codeword $c^{(i)} \in F^n$ (or, equivalently, the error pattern $e^{(i)} = y^{(i)} - c^{(i)}$). In this case, Forney's formula (107) can be applied directly, and it is often more attractive than first finding $a^{(i)}(x)$ and then computing $c^{(i)} = \psi(a^{(i)}(x))$.

VII. ANALYSIS OF THE ERROR-LOCATING ALGORITHM

This section gives a detailed analysis of the SPI error-locating algorithm presented in Section VI. (The extension to the case where each row code has different dimension k is addressed in Appendix A).

A. Guaranteed Error-Locating Capability

Our main result here is Theorem 5, which was stated in Section VI and will now be proved. To this end, we will need the following Theorem 9, which is inspired by [10], [16], [17], and similar (but not identical) to Lemma 3 of [10]; on the other hand, it generalizes Theorem 1 of [3].

Theorem 9. If

$$2|U_E| \leq n - k + r_E - 1, \quad (137)$$

then the error locator polynomial (102) satisfies

$$\deg(Y^{(i)}(x)\Lambda_E(x) \bmod m(x)) < \frac{n + k + r_E - 1}{2} \quad (138)$$

for all $i \in \{1, \dots, L\}$. Conversely, for any Y and any $E \in F^{L \times n}$ (of rank r_E) and $t \in \mathbb{R}$ with

$$|U_E| \leq t \leq \frac{n - k + r_E - 1}{2} \quad (139)$$

if some nonzero $\Lambda(x) \in F[x]$ with $\deg \Lambda(x) \leq t$ satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < n - t + r_E - 1 \quad (140)$$

for all $i \in \{1, \dots, L\}$, then $\Lambda(x)$ is a multiple of $\Lambda_E(x)$. \square

The proof is given below. In the special case where $L = 1$, we have $r_E = 1$ (if $|U_E| > 0$) and the theorem reduces to Theorem 1 of [3].

Corollary 1. Assume that (137) holds. If some nonzero $\Lambda(x) \in F[x]$ with $\deg \Lambda(x) \leq |U_E|$ satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k + |U_E| \quad (141)$$

for all $i \in \{1, \dots, L\}$, then $\Lambda(x) = \gamma \Lambda_E(x)$ for some nonzero $\gamma \in F$. \square

Proof: Using (137), we have

$$k + |U_E| \leq k + (n - k + r_E - 1 - |U_E|) \quad (142)$$

$$= n - |U_E| + r_E - 1. \quad (143)$$

A polynomial $\Lambda(x)$ satisfying (141) thus satisfies (140) with $t = |U_E|$, and thus $\Lambda(x)$ is a multiple of $\Lambda_E(x)$. But $\deg \Lambda(x) \leq |U_E| = \deg \Lambda_E(x)$, and $\Lambda(x) = \gamma \Lambda_E(x)$ follows. \blacksquare

Note that (137) agrees with (114), and (141) agrees with (110). Theorem 5 then follows from Corollary 1.

Proof of Theorem 9: The direct part is easy: (109) and (137) implies $k + |U_E| \leq \frac{n+k+r_E-1}{2}$.

For the converse, assume (139), (140), and $\deg \Lambda(x) \leq t$, and consider

$$Y^{(i)}(x)\Lambda(x) \bmod m(x) = C^{(i)}(x)\Lambda(x) + E^{(i)}(x)\Lambda(x) \bmod m(x). \quad (144)$$

Under the stated assumptions, the degree of the left-hand side of (144) is smaller than $n - t + r_E - 1$ and also

$$\deg(C^{(i)}(x)\Lambda(x)) < k + t \leq n - t + r_E - 1. \quad (145)$$

It follows that

$$\deg(E^{(i)}(x)\Lambda(x) \bmod m(x)) < n - t + r_E - 1 \quad (146)$$

for all $i \in \{1, \dots, L\}$.

Now, let $\tilde{Y}(x) \triangleq \sum_{i=1}^L q_i Y^{(i)}(x)$ where $q_i \in F$. We then have

$$\tilde{Y}(x) = \tilde{C}(x) + \tilde{E}(x) \quad (147)$$

where $\tilde{C}(x) \triangleq \sum_{i=1}^L q_i C^{(i)}(x)$ satisfies $\deg \tilde{C}(x) < k$, and where

$$\tilde{E}(x) \triangleq \sum_{i=1}^L q_i E^{(i)}(x) \quad (148)$$

satisfies

$$\deg(\tilde{E}(x)\Lambda(x) \bmod m(x)) < n - t + r_E - 1. \quad (149)$$

Also, let $\tilde{e} \triangleq \psi(\tilde{E}(x)) = (\tilde{e}_1, \dots, \tilde{e}_n) \in F^n$ with ψ as in (96), and let $\tilde{U} \subset \{1, \dots, n\}$ be the set indexing the nonzero entries of \tilde{e} . We then have $\tilde{e} = \sum_{i=1}^L q_i e^{(i)}$ and $\tilde{U} \subseteq U_E$ for any choice of q_1, \dots, q_L . Furthermore, we define

$$\tilde{\Lambda}_E(x) \triangleq \prod_{j \in \tilde{U}} (x - \beta_j). \quad (150)$$

Clearly, $\deg \tilde{\Lambda}_E(x) = |\tilde{U}|$, and $\tilde{\Lambda}_E(x)$ divides $\Lambda_E(x)$.

Since E has rank r_E , we can choose the values of q_1, \dots, q_L such that $\tilde{e} = \psi(\tilde{E}(x)) \in F^n$ has exact $|\tilde{U}| = |U_E| - r_E + 1$ nonzero entries for some $\tilde{U} \subset U_E$. We then write

$$\tilde{E}(x)\Lambda(x) = g(x)m(x) + \tilde{E}(x)\Lambda(x) \bmod m(x) \quad (151)$$

according to the polynomial division theorem. But $\tilde{E}(x)$ (and thus $\tilde{E}(x)\Lambda(x)$) has at least

$$n - |\tilde{U}| = n - |U_E| + r_E - 1 \geq n - t + r_E - 1 \quad (152)$$

zeros in the set $\{\beta_0, \beta_1, \dots, \beta_{n-1}\}$. It follows that $\tilde{E}(x)\Lambda(x) \bmod m(x)$ has also at least $n - t + r_E - 1$ zeros (in this set), which contradicts (149) unless

$$\tilde{E}(x)\Lambda(x) \bmod m(x) = 0. \quad (153)$$

Therefore, $\Lambda(x)$ satisfies (153).

But any such nonzero $\Lambda(x)$ that satisfies (153) is a multiple of the polynomial $\tilde{\Lambda}_E(x)$. It follows that $\Lambda(x)$ must be a multiple of $\Lambda_E(x)$ because $\Lambda(x)$ is a multiple of $\tilde{\Lambda}_E(x)$ for every $\tilde{U} \subset U_E$ with $|\tilde{U}| = |U_E| - r_E + 1$. \square

We now turn to prove Propositions 6 and 7.

Proof of Proposition 6: Assume that (117) holds and consider the very first test of (112), where $\tau^{(i)} = n - 1$, $i = 1, \dots, L$. We then have

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < n - 1 \quad (154)$$

with $\deg \Lambda(x) \leq \deg \Lambda_E(x) = |U_E|$. Then (140) is satisfied with $t = |U_E|$, and it follows that $\Lambda(x) = \gamma \Lambda_E(x)$. Thus $\Lambda(x)$ passes the test (112) and the algorithm stops. \square

Proof of Proposition 7: Suppose $L \geq |U_E| > 0$. It is easily seen that

$$\Pr(r_E = |U_E|) = \frac{(q^L - 1)(q^L - q) \cdots (q^L - q^{|U_E|-1})}{(q^L - 1)^{|U_E|}} \quad (155)$$

$$= \frac{(q^L - q) \cdots (q^L - q^{|U_E|-1})}{(q^L - 1)^{|U_E|-1}} \quad (156)$$

where the numerator of (155) is the number of ways of picking $|U_E|$ linearly independent column vectors.

Note that the numerator of (156) equals

$$q^{L(|U_E|-1)} (1 - q^{-(L-1)}) \cdots (1 - q^{-(L-|U_E|+1)}); \quad (157)$$

we then have

$$\Pr(r_E = |U_E|) > (1 - q^{-(L-1)}) \cdots (1 - q^{-(L-|U_E|+1)}). \quad (158)$$

We can go further to get the weaker (looser) bound

$$\Pr(r_E = |U_E|) > 1 - \sum_{i=1}^{|U_E|-1} q^{-(L-i)} \quad (159)$$

and then obtain

$$\Pr(r_E \neq |U_E|) < \sum_{i=1}^{|U_E|-1} q^{-(L-i)} \quad (160)$$

$$< \frac{q^{-(L-|U_E|)}}{q-1} \quad (161) \quad \square$$

B. Statistical Error-Locating Capability

Our main result here is Theorem 6, which was stated in Section VI. As we have seen, the key to Theorem 6 is Lemma 4, which will be proved now.

The proof of Lemma 4 starts with the following fact.

Proposition 8. If $\Lambda(x) = \Lambda_E(x)$ does not solve the SPI problem (110), then there exists some nonzero polynomial $\Lambda(x)$ such that $\deg \Lambda(x) < |U_E|$ and

$$\deg(E^{(i)}(x)\Lambda(x) \bmod m(x)) < k + |U_E| \quad (162)$$

for all $i = 1, \dots, L$. \square

Let U be an arbitrary, but fixed, subset of $\{0, \dots, n-1\}$, and assume that the $|U|$ nonzero columns of the $L \times n$ matrix E are uniformly and independently distributed over $F^L \setminus \{0\}$. In the following, we denote U_E by U and denote $|U_E|$ by $|U|$ (for simplicity of the notation).

Let S_U be the set of all the possible error matrices E with the given support set U . Let $S_f \subset S_U$ be the set of all $E \in S_U$

that admit some $\Lambda(x) \in F[x]$ with $0 \leq \deg \Lambda(x) < |U|$ that satisfies (162) for all $i \in \{1, \dots, L\}$. Then,

$$P_\Lambda \leq \frac{|S_f|}{|S_U|} = \frac{|S_f|}{(q^L - 1)^{|U|}} \quad (163)$$

It thus remains to bound $|S_f|$.

For $t = 0, \dots, |U| - 1$, let \mathcal{L}_t be the set of monic polynomials $\Lambda(x) \in F[x]$ with $\deg \Lambda(x) < |U|$ and with exactly t zeros in the set $\mathcal{B}_U \triangleq \{\beta_\ell : \ell \in U\}$.

Lemma 9. For any fixed $\Lambda(x) \in \mathcal{L}_t$, the number of error patterns $E \in S_U$ that satisfy (162) is upper bounded by $q^{L(2|U|-(n-k)-t)}$. \square

The proof will be given below. We then have

$$|S_f| \leq \sum_{t=0}^{|U|-1} |\mathcal{L}_t| q^{L(2|U|-(n-k)-t)}. \quad (164)$$

Lemma 10.

$$|\mathcal{L}_t| = \binom{|U|}{t} (q-1)^{|U|-t-1}. \quad (165)$$

The proof is given below. Thus (164) becomes

$$|S_f| \leq \sum_{t=0}^{|U|-1} \binom{|U|}{t} (q-1)^{|U|-t-1} q^{L(2|U|-(n-k)-t)} \quad (166)$$

$$= w \sum_{t=0}^{|U|-1} \binom{|U|}{t} (q-1)^{-t} q^{-Lt} \quad (167)$$

$$< w \sum_{t=0}^{|U|} \binom{|U|}{t} ((q-1)^{-1} q^{-L})^t \quad (168)$$

$$= w(1 + (q-1)^{-1} q^{-L})^{|U|} \quad (169)$$

$$= \frac{q^{L(|U|-(n-k))}}{q-1} ((q-1)q^L + 1)^{|U|} \quad (170)$$

with

$$w \triangleq (q-1)^{|U|-1} q^{L(2|U|-(n-k))} \quad (171)$$

in (167)–(169). From (163), we then have

$$P_\Lambda < \frac{q^{L(|U|-(n-k))}}{q-1} \left(\frac{q^{L+1} - q^L + 1}{q^L - 1} \right)^{|U|} \quad (172)$$

$$= \frac{q^{-L(n-k-|U|)+|U|}}{q-1} \left(\frac{q^L - (q^{L-1} - q^{-1})}{q^L - 1} \right)^{|U|} \quad (173)$$

and (119) follows if $L > 1$.

For the proof of Lemma 9, we will use the following elementary fact.

Proposition 9. The number of nonzero polynomials over F of degree at most ν and with $\mu \leq \nu$ prescribed zeros in F (and allowing additional zeros in F) is $|F|^{\nu-\mu+1} - 1$. \square

Proof of Lemma 9: Consider the polynomial $\tilde{E}^{(i)}(x) = \psi^{-1}(e^{(i)})$ where $e^{(i)}$ is a row of E , and let $\tilde{E}^{(i)}(x) \triangleq E^{(i)}(x)\Lambda(x) \bmod m(x)$. From (96), we have

$$\tilde{E}^{(i)}(\beta_\ell) = e_{i,\ell} \Lambda(\beta_\ell) \quad (174)$$

where $e_{i,\ell}$ denotes the element in row i and column ℓ of E . From (162), we have $\deg \tilde{E}^{(i)}(x) < k + |U|$. But (174) implies that $\tilde{E}^{(i)}(x)$ has at least $n - |U| + t$ zeros in prescribed positions: $e_{i,\ell} = 0$ for $\ell \notin U$ and $\Lambda(x)$ has t zeros in $\mathcal{B}_U = \{\beta_\ell : \ell \in U\}$. By Proposition 9, the number of such polynomials $\tilde{E}^{(i)}$ is bounded by $q^{2|U|-(n-k)-t}$, and putting all rows together yields the lemma. \square

Proof of Lemma 10: Consider nonzero polynomials $\Lambda(x) \in F[x]$ with $\deg \Lambda(x) < |U|$ and with t prescribed zeros in $\mathcal{B}_U (= \{\beta_\ell : \ell \in U\})$ and no other zeros in \mathcal{B}_U . The number of such polynomials $\Lambda(x)$ is $(q-1)^{|U|-t}$, as is obvious from the ring isomorphism

$$F[x]/m_U(x) \rightarrow F^{|U|} : \Lambda(x) \mapsto (\Lambda(\beta'_1), \dots, \Lambda(\beta'_{|U|})) \quad (175)$$

with $m_U(x) \triangleq \prod_{\ell \in U} (x - \beta_\ell)$ and $\{\beta'_1, \dots, \beta'_{|U|}\} \triangleq \mathcal{B}_U$. Lemma 10 then follows from noting that it counts only monic polynomials. \square

VIII. PROOF OF THE SPI ALGORITHM

We first prove Lemma 1; then proceed to prove Theorem 2. (Algorithms 2 and 3 are easy modifications of Algorithm 1 and do not require an extra proof.)

A. Proof of Lemma 1

First, $\delta_{\max}(\Lambda') \geq \delta_{\max}(\Lambda'')$ is obvious from the assumptions. From (80), we obtain

$$r(x) \triangleq b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x) \quad (176)$$

$$= \kappa'' r'(x) - \kappa' x^{d'-d''} r''(x) \quad (177)$$

with

$$r'(x) \triangleq b^{(i)}(x)\Lambda'(x) \bmod m^{(i)}(x) \quad (178)$$

$$r''(x) \triangleq b^{(i)}(x)\Lambda''(x) \bmod m^{(i)}(x) \quad (179)$$

by the natural ring homomorphism $F[x] \rightarrow F[x]/m^{(i)}(x)$. It is then obvious from (177) that $\deg r(x) < \deg r'(x) = d'$, which is (81).

For the remaining proof, we define

$$\delta^{(\ell)}(\Lambda) \triangleq \text{rd}^{(\ell)}(\Lambda) - \tau^{(\ell)} \quad (180)$$

for every $\ell \in \{1, \dots, L\}$. With this notation, we have

$$\delta^{(i)}(\Lambda) < \delta^{(i)}(\Lambda') \quad (181)$$

from (81). We will next show that

$$\delta^{(j)}(\Lambda) \leq \delta^{(i)}(\Lambda') \text{ for } j < i \quad (182)$$

and

$$\delta^{(k)}(\Lambda) < \delta^{(i)}(\Lambda') \text{ for } k > i. \quad (183)$$

Clearly, (181)–(183) together imply both (82) and either (83) or (84) (or both).

To this end, we first note that $d' - d'' = \delta^{(i)}(\Lambda') - \delta^{(i)}(\Lambda'')$, and thus

$$d' - d'' + \delta^{(i)}(\Lambda'') = \delta^{(i)}(\Lambda'). \quad (184)$$

We then note from (80) that

$$\delta^{(\ell)}(\Lambda) \leq \max \left\{ \delta^{(\ell)}(\Lambda'), d' - d'' + \delta^{(\ell)}(\Lambda'') \right\} \quad (185)$$

for every $\ell \in \{1, \dots, L\}$.

Concerning (182), the assumption $i_{\max}(\Lambda') = i$ implies

$$\delta^{(j)}(\Lambda') \leq \delta^{(i)}(\Lambda') \quad (186)$$

for every $j < i$, and $i_{\max}(\Lambda'') = i$ implies

$$\delta^{(j)}(\Lambda'') \leq \delta^{(i)}(\Lambda''). \quad (187)$$

It then follows from (185)–(187) that for all $j < i$

$$\delta^{(j)}(\Lambda) \leq \max \left\{ \delta^{(i)}(\Lambda'), d' - d'' + \delta^{(i)}(\Lambda'') \right\}, \quad (188)$$

and (182) follows from (184).

Concerning (183), the assumption $i_{\max}(\Lambda') = i$ implies

$$\delta^{(k)}(\Lambda') < \delta^{(i)}(\Lambda') \quad (189)$$

for every $k > i$, and $i_{\max}(\Lambda'') = i$ implies

$$\delta^{(k)}(\Lambda'') < \delta^{(i)}(\Lambda''). \quad (190)$$

It then follows from (185), (189), and (190) that for all $k > i$

$$\delta^{(k)}(\Lambda) < \max \left\{ \delta^{(i)}(\Lambda'), d' - d'' + \delta^{(i)}(\Lambda'') \right\}, \quad (191)$$

and (183) follows from (184).

B. Assertions

For the detailed proof, we annotate the basic algorithm of Section IV with some extra variables and some assertions as shown in Algorithm 7. We will prove these assertions one by one, except that the proof of Assertion (A.1) is deferred to the end of this section.

Assertion (A.2) is obvious both from the initialization and from (A.11). Assertion (A.3) is the result of the **repeat** loop, as discussed at the beginning of Section IV-A.

Assertion (A.4) is obvious. Assertions (A.5)–(A.8) follow from (A.2)–(A.4), followed by the swap in lines 21–23.

As for (A.9), when $b^{(i)}(x)$ is visited for the very first time (i.e., the first execution of line 26 for some index i), we have $d = \deg m^{(i)}(x)$ and $\text{rd}^{(i)}(\Lambda) < d$ is obvious. For all later executions of line 26, we have $d = \text{rd}^{(i)}(\Lambda)$ and $d^{(i)} = \text{rd}^{(i)}(\Lambda^{(i)})$ before line 26, and $\text{rd}^{(i)}(\Lambda) < d$ after line 26 follows from Lemma 1.

In order to prove (A.10) and (A.11), we need to understand how line 26 changes the degree of $\Lambda(x)$.

Lemma 11. Line 26 changes the degree of $\Lambda(x)$ only in iterations where lines 21–24 are executed. \square

The proof is given in Section VIII-D below.

If lines 21–24 are executed, then line 26 changes the degree of $\Lambda(x)$ to

$$\deg \Lambda^{(i)}(x) + d - d^{(i)} = \deg \Lambda_k(x) + \Delta_k, \quad (192)$$

which is (A.10). With (A.7), the left-hand side of (192) yields also (A.11).

It remains to prove (A.1). First, we note that (A.1) clearly holds when the **loop** is entered for the first time. But if (A.1) holds, then $\Lambda^{(i)}(x)$ in (A.6) satisfies

$$\begin{aligned} \deg \Lambda^{(i)}(x) &= \sum_{j \neq i}^L (\deg m^{(j)}(x) - d^{(j)}) \\ &\quad + \deg m^{(i)}(x) - d. \end{aligned} \quad (193)$$

Algorithm 7

Annotated SPI Algorithm

```

1  for  $i = 1, \dots, L$  begin
2     $\Lambda^{(i)}(x) := 0$ 
3     $d^{(i)} := \deg m^{(i)}(x)$ 
4     $\kappa^{(i)} := \text{lcf } m^{(i)}(x)$ 
5  end
6   $\Lambda(x) := 1$ 
7   $\delta := \max_{i \in \{1, \dots, L\}} (\deg m^{(i)}(x) - \tau^{(i)})$ 
8   $i := 1$ 

```

Extra:
 $k := 0$ (E.1)

```

9  loop begin

```

Assertions:
 $\deg \Lambda(x) = \sum_{i=1}^L (\deg m^{(i)}(x) - d^{(i)})$ (A.1)
 $\deg \Lambda(x) > \deg \Lambda^{(i)}(x), \quad i = 1, \dots, L$ (A.2)

```

10 repeat
11   if  $i > 1$  begin  $i := i - 1$  end
12   else begin
13     if  $\delta \leq 0$  return  $\Lambda(x)$ 
14      $i := L$ 
15      $\delta := \delta - 1$ 
16   end
17    $d := \delta + \tau^{(i)}$ 
18    $\kappa := \text{coefficient of } x^d \text{ in}$ 
19      $b^{(i)}(x)\Lambda(x) \bmod m^{(i)}(x)$ 
20 until  $\kappa \neq 0$ 

```

Assertion:
 $i = i_{\max}(\Lambda), \delta = \delta_{\max}(\Lambda) \geq 0$ (A.3)

```

21 if  $d < d^{(i)}$  begin

```

Assertion:
 $d^{(i)} > d = \delta + \tau^{(i)} \geq \tau^{(i)}$ (A.4)
Extras:
 $k := k + 1, i_k \triangleq i, \Lambda_k(x) \triangleq \Lambda(x),$
 $\Delta_k \triangleq d^{(i)} - d, d_k \triangleq d^{(i)}$ (E.2)

```

22   swap  $(\Lambda(x), \Lambda^{(i)}(x))$ 
23   swap  $(d, d^{(i)})$ 
24   swap  $(\kappa, \kappa^{(i)})$ 
25    $\delta := d - \tau^{(i)}$ 

```

Assertions:
 $d > d^{(i)} \geq \tau^{(i)}$ (A.5)
 $\deg \Lambda^{(i)}(x) > \deg \Lambda(x)$ (A.6)
 $\deg \Lambda^{(i)}(x) > \deg \Lambda^{(j)}(x)$ for $j \neq i$ (A.7)
 $i_{\max}(\Lambda^{(i)}) = i, \delta_{\max}(\Lambda^{(i)}) \geq 0$ (A.8)

```

26   end
27    $\Lambda(x) := \kappa^{(i)}\Lambda(x) - \kappa x^{d-d^{(i)}}\Lambda^{(i)}(x)$ 

```

Assertions:
 $\text{rd}^{(i)}(\Lambda) < d = \delta + \tau^{(i)}$ (A.9)
 $\deg \Lambda(x) = \Delta_k + \deg \Lambda_k(x)$ (A.10)
 $> \deg \Lambda^{(i)}(x), \quad i = 1, \dots, L$ (A.11)

```

28 end

```

It then follows from (192) that $\Lambda(x)$ after line 26 satisfies

$$\deg \Lambda^{(i)}(x) + d - d^{(i)} = \sum_{j=1}^L (\deg m^{(j)}(x) - d^{(j)}), \quad (194)$$

which is (A.1).

For later use, we also record the following fact from (E.2) and (A.10):

Proposition 10. The polynomials $\Lambda_k(x)$ defined in (E.2) satisfy $\deg \Lambda_1(x) = 0$ (since $\Lambda_1(x) = 1$) and

$$\deg \Lambda_k(x) > \dots > \deg \Lambda_2(x) > \deg \Lambda_1(x) \quad (195)$$

with

$$\deg \Lambda_{t+1}(x) = \Delta_t + \deg \Lambda_t(x) \quad (196)$$

for $1 \leq t < K$. \square

Finally, we note that the algorithm is guaranteed to terminate because every execution of the **repeat** loop (lines 10–19) strictly decreases $\delta_{\max}(\Lambda)$ or $i_{\max}(\Lambda)$ according to Lemma 1 and the swap in lines 21–23 strictly decreases $d^{(i)}$.

C. Proving the Minimality of the Returned $\Lambda(x)$

Let $\Lambda(x)$ be the polynomial that is returned by the algorithm. It is clear at this point that $\Lambda(x)$ satisfies (1) for all $i \in \{1, \dots, L\}$. It remains to prove that no polynomial of smaller degree satisfies (1) for all i . The proof involves several steps.

Let $\Lambda_1(x), \Lambda_2(x), \dots, \Lambda_K(x)$ be all polynomials $\Lambda_k(x)$ from (E.2) and note that $\deg \Lambda(x) > \deg \Lambda_K(x)$.

Lemma 12. Any nonzero $\tilde{\Lambda}(x) \in F[x]$ with $\deg \tilde{\Lambda}(x) < \deg \Lambda(x)$ can be uniquely written as

$$\tilde{\Lambda}(x) = \sum_{k=1}^K q_k(x) \Lambda_k(x) \quad (197)$$

with polynomials $q_k(x)$ such that

$$\deg q_k(x) < \deg \Lambda_{k+1}(x) - \deg \Lambda_k(x) \quad (198)$$

for $k = 1, \dots, K-1$, and

$$\deg q_K(x) < \deg \Lambda(x) - \deg \Lambda_K(x). \quad (199)$$

\square

The lemma is obvious from dividing $\tilde{\Lambda}(x)$ successively by $\{\Lambda_K(x), \Lambda_{K-1}(x), \dots, \Lambda_1(x) = 1\}$.

In the following, we will work towards proving that any nonzero polynomial $\tilde{\Lambda}(x)$ as in Lemma 12 satisfies $\delta_{\max}(\tilde{\Lambda}) \geq 0$, which implies that $\tilde{\Lambda}(x)$ cannot not satisfy (1) for all $i \in \{1, \dots, L\}$.

To this end, we need to study the values of $i_{\max}(q_k \Lambda_k)$ and $\delta_{\max}(q_k \Lambda_k)$. We begin by noting (from (A.3) and (E.2)) that

$$i_{\max}(\Lambda_k) = i_k \text{ and } \delta_{\max}(\Lambda_k) \geq 0 \quad (200)$$

for all $k \in \{1, \dots, K\}$.

From Proposition 10, we have

$$\Delta_k = \deg \Lambda_{k+1}(x) - \deg \Lambda_k(x) \quad (201)$$

for $k \in \{1, \dots, K-1\}$ and

$$\Delta_K = \deg \Lambda(x) - \deg \Lambda_K(x). \quad (202)$$

We then obtain from (198)–(202) that

$$\deg q_k(x) < \Delta_k \quad (203)$$

for all $k \in \{1, \dots, K\}$.

On the other hand, we have from (E.2) that

$$\Delta_k = d_k - \deg(b^{(i_k)}(x) \Lambda_k(x) \bmod m^{(i_k)}(x)) \quad (204)$$

for $k = 1, 2, \dots, K$. We then obtain from (203) and (204) that

$$\deg q_k(x) + \deg(b^{(i_k)}(x) \Lambda_k(x) \bmod m^{(i_k)}(x)) < d_k \quad (205)$$

for $k = 1, 2, \dots, K$.

Lemma 13. For any nonzero $q_k(x)$, we have

$$i_{\max}(q_k \Lambda_k) = i_{\max}(\Lambda_k) \quad (206)$$

and

$$\delta_{\max}(q_k \Lambda_k) = \deg q_k(x) + \delta_{\max}(\Lambda_k). \quad (207)$$

\square

Proof: For all $i \in \{1, \dots, L\}$, we clearly have

$$\text{rd}^{(i)}(q_k \Lambda_k) \leq \deg q_k + \text{rd}^{(i)}(\Lambda_k). \quad (208)$$

For i_k , however, we have

$$\text{rd}^{(i_k)}(q_k \Lambda_k) = \deg q_k + \text{rd}^{(i_k)}(\Lambda_k) \quad (209)$$

from (205) and since $d_k \leq \deg m^{(i_k)}(x)$. The lemma then follows from $i_{\max}(\Lambda_k) = i_k$. \blacksquare

In the next step, we partition the indices $k \in \{1, \dots, K\}$ into sets S_1, \dots, S_L such that

$$k \in S_i \iff i_{\max}(\Lambda_k) = i_k = i. \quad (210)$$

We then write (197) as

$$\tilde{\Lambda}(x) = \sum_{i=1}^L \left(\sum_{k \in S_i} q_k(x) \Lambda_k(x) \right) \quad (211)$$

$$= \sum_{i=1}^L \tilde{\Lambda}^{(i)}(x) \quad (212)$$

with

$$\tilde{\Lambda}^{(i)}(x) \triangleq \sum_{k \in S_i} q_k(x) \Lambda_k(x). \quad (213)$$

Lemma 14. If $\tilde{\Lambda}^{(i)}(x)$ is nonzero, then

$$i_{\max}(\tilde{\Lambda}^{(i)}) = i \quad (214)$$

and

$$\delta_{\max}(\tilde{\Lambda}^{(i)}) \geq 0. \quad (215)$$

\square

The proof is given below. Consider now the mapping

$$\varphi : \tilde{\Lambda}(x) \mapsto (\varphi_1(\tilde{\Lambda}), \dots, \varphi_L(\tilde{\Lambda})) \quad (216)$$

where φ_i is the mapping

$$\tilde{\Lambda}(x) \mapsto r^{(i)}(x) \triangleq b^{(i)}(x)\tilde{\Lambda}(x) \bmod m^{(i)}(x) \quad (217)$$

$$\mapsto (r_0^{(i)}, \dots, r_{\deg m^{(i)}(x)-1}^{(i)}) \quad (218)$$

$$\mapsto (r_{\tau^{(i)}}^{(i)}, \dots, r_{\deg m^{(i)}(x)-1}^{(i)}). \quad (219)$$

Note that $\tilde{\Lambda}(x)$ satisfies (1) if and only if $\tilde{\Lambda}(x) \in \ker \varphi$. Since φ is linear, we have

$$\varphi(\tilde{\Lambda}) = \sum_{i=1}^L \varphi(\tilde{\Lambda}^{(i)}). \quad (220)$$

But (215) implies that $\varphi(\tilde{\Lambda}^{(i)})$ is nonzero if and only if $\tilde{\Lambda}^{(i)}(x)$ is nonzero, and (214) implies that the nonzero elements in the list $\varphi(\tilde{\Lambda}^{(1)}), \dots, \varphi(\tilde{\Lambda}^{(L)})$ are linearly independent. It follows that (220) cannot be zero (for any nonzero $\tilde{\Lambda}(x)$ as in Lemma 12), which means that $\tilde{\Lambda}(x)$ does not satisfy (1) for all $i \in \{1, \dots, L\}$.

Proof of Lemma 14:

We clearly have

$$\delta_{\max}(\tilde{\Lambda}^{(i)}) \leq \max_{k \in S_i} \delta_{\max}(q_k \Lambda_k). \quad (221)$$

We show equality in (221) by showing that

$$\text{rd}^{(i)}\left(\sum_{k \in S_i} q_k(x) \Lambda_k(x)\right) = \max_{k \in S_i} \text{rd}^{(i)}(q_k \Lambda_k). \quad (222)$$

For any $k, k' \in S_i$ with $k < k'$, we have

$$\deg m^{(i)}(x) \geq d_k > d_{k'} \geq \tau^{(i)} \quad (223)$$

and

$$\text{rd}^{(i)}(q_k \Lambda_k) \geq \text{rd}^{(i)}(\Lambda_k) \geq d_{k'} \quad (224)$$

and

$$\text{rd}^{(i)}(q_k \Lambda_k) = \deg q_k(x) + \text{rd}^{(i)}(\Lambda_k) < d_k \quad (225)$$

from (209) and (205). It follows that

$$\max_{k \in S_i} \text{rd}^{(i)}(q_k \Lambda_k) = \text{rd}^{(i)}(q_\ell \Lambda_\ell) \quad (226)$$

with $\ell \triangleq \min\{k \in S_i : q_k(x) \neq 0\}$, and (222) is obvious. From (221) and (222), we also have (214), and (215) is obvious from (222)–(224). \square

D. Proof of Lemma 11

Lemma 11 is, in fact, a consequence of (A.6), (A.7), (192), Lemma 1, and the fact that $\Lambda^{(i)}(x)$ for all i remain unchanged between consecutive executions of lines 21–24. In the following, we elaborate the fact by induction.

Let k denote the k -th execution of lines 21–24, and let $i_{k,n}$ and $\delta_{k,n}$ denote the respective values of i and $d - d^{(i)}$ of the n -th execution of line 26 *after* the present and *before* the $(k+1)$ -th execution of lines 21–24. We gather the executions of line 26 (between the k -th and $(k+1)$ -th executions of lines 21–24) into a group, called the k -th group; clearly, for the k -th group, we have $i_{k,1} = i_k$ and $\delta_{k,1} = \Delta_k$ of (E.2).

To prove the lemma is equivalent to prove the statement: subsequent executions of line 26 in the present group do not change the degree of $\Lambda(x)$.

As an inductive hypothesis, we assume that $\deg \Lambda(x)$ only changes in the first execution of line 26 of every previous group before k , and assume that $\deg \Lambda(x)$ remains the same before executing the upcoming n -th ($n \geq 2$) execution of line 26 of the k -th group.

We will verify that $\deg \Lambda(x)$ remains unchanged in the n -th ($n \geq 2$) execution of line 26 (of the k -th group) in all possible cases; these cases can be deduced from (81)–(84) of Lemma 1.

Note first the fact that $\Lambda^{(i)}(x)$ for any $i \in \{1, \dots, L\}$ is never changed inside the k -th group.

Case 1: if $i_{k,n} = i_{k,n-1}$, then from the inductive hypothesis and from that $\Lambda^{(i_{k,n})}(x)$ remains unchanged inside the k -th group, and from the fact that $\delta_{k,n} < \delta_{k,n-1} \leq \delta_{k,1}$ because of (81), we see that line 26 does not increase $\deg \Lambda(x)$; if $L = 1$, the proof is completed here as in [3], [4].

In the following, we consider different cases where $i_{k,n} \neq i_{k,n-1}$. Note that if $i_{k,n} \neq i_{k,n-1}$, the $\Lambda^{(i_{k,n})}(x)$ involved in line 26 must be such that its *first* execution of line 26 has appeared in “some” previous group that is *closest* to the present k -th group.

Case 2: suppose $i_{k,n} \neq i_{k,n-1}$, and let us say this is the *very first* revisit of the same $i_{k,n}$ since that “some” previous (closest) group. We then note that in the present group, the *net* increase of $d = \text{rd}^{(i_{k,n})}(\Lambda)$ is never larger than $\delta_{k,1}$ because of (82). It then follows from the inductive hypothesis that for each previous group, say the ν -th group, the *net* increase of $\text{rd}^{(i_{k,n})}(\Lambda)$ in that group is never larger than the corresponding $\delta_{\nu,1}$ (because of (81)–(84)), and thus the *accumulation* of the net increase of $\text{rd}^{(i_{k,n})}(\Lambda)$ from the “some” to the present group is never larger than the corresponding *accumulation* of the net increase of $\deg \Lambda(x)$ from these groups. Together with the fact that $\Lambda^{(i_{k,n})}(x)$ remains the same from that “some” previous (closest) group, we can see that $\deg \Lambda(x)$ does not change in this case.

Case 3: suppose $i_{k,n} \neq i_{k,n-1}$, and let us say that this is a second revisit of $b^{(i_{k,n})}(x)$ in the present group. For this case, line 26 does not change $\deg \Lambda(x)$ because of (81)–(84) and because of the same $\Lambda^{(i_{k,n})}(x)$ as in Case 1.

Case 4: suppose $i_{k,n} \neq i_{k,n-1}$, and let us say that this is a first revisit of $b^{(i_{k,n})}(x)$ in the present group, and say that $b^{(i_{k,n})}(x)$ has been revisited in the groups between that “some” (closest) group and the present one. This case can be viewed as a continuation of Cases 2 and 3, i.e., Cases 2 and 3 already appeared in the previous groups. But even though, we still have, in the present group, $\delta_{k,n} \leq \delta_{k,1}$ from (81)–(84). Then from the inductive hypothesis and the fact that $\Lambda^{(i_{k,n})}(x)$ is not changed (since that “some” closest group), we learn that line 26 does not change $\deg \Lambda(x)$.

From Cases 1–4, we conclude that in any case $\deg \Lambda(x)$ does not change in the n -th execution of the k -th group. The equivalent “statement” (and thus Lemma 11) then follows by induction.

IX. CONCLUSION

We have introduced the simultaneous partial-inverse problem for polynomials mod $m^{(i)}(x)$, which generalizes the partial-inverse problem to the multi-sequence setting. In contrast to the MSSRS problem, the SPI problem has always

a unique solution (up to a scale factor) and comes with a nontrivial upper bound on the degree of the solution. These two properties play a key role throughout the paper.

We have presented a new algorithm for solving the SPI problem, which strongly resembles the multi-sequence Berlekamp-Massey algorithm. We also give two variations of the basic algorithm, but these variations appear less attractive in the multi-sequence setting than in the single sequence setting of [4]. We have also shown that the SPI problem with general moduli $m^{(i)}(x)$ can be efficiently transformed into a SPI problem with moduli of the form $m^{(i)}(x) = x^{\nu^{(i)}}$ and thus efficiently solved by the proposed SPI algorithm. (To the best of our knowledge, no such transformation has been reported in the prior literature on interleaved Reed-Solomon codes.)

We have shown that decoding interleaved Reed-Solomon codes and subfield evaluation codes can be naturally reduced to several different SPI problems and decoded by obvious adaptations of the SPI algorithms. The resulting algorithms are very efficient, and they achieve both the best bound for guaranteed error correction (using the rank of the error matrix) and the best bound on failure probability for random errors; this combination has not previously been reported in the literature.

In the appendix, we generalize these decoding algorithms and their analysis to array codes with row codes of different dimensions.

APPENDIX A APPLICATION TO DECODING HETEROGENEOUS INTERLEAVED REED-SOLOMON CODES

We now consider the heterogeneous interleaved Reed-Solomon codes as in [8] where row codes can have different dimension k . We will parallel the presentation in Section VI, and we will see that the many results in Sections VI and VII generalize straightforward to such array codes.

A. The Heterogeneous Array Codes

Let F be a finite field. Let $\mathcal{C}_{\text{HIRS}}$ denote an array code where codewords are $L \times n$ arrays over F such that each row i is a codeword from an $(n, k^{(i)})$ Reed-Solomon codes, i.e., the row code for i -th row is defined as the set

$$\{c \in F^n : \deg \psi^{-1}(c) < k^{(i)}\} \quad (227)$$

with ψ as in (96). In general, $k^{(i)}$ can be different, and we define

$$k_{\max} \triangleq \max\{k^{(i)}, 1 \leq i \leq L\} \quad (228)$$

and

$$k_{\text{avg}} \triangleq \frac{1}{L} \sum_{i=1}^L k^{(i)} \quad (229)$$

If $k^{(i)} = k$ for all i , then $k_{\max} = k_{\text{avg}} = k$, and $\mathcal{C}_{\text{HIRS}}$ reduces to an array code as in Section V.

We define error locator polynomial $\Lambda_E(x)$ as in (102), which satisfies $\deg \Lambda_E(x) = |U_E|$ and (108).

If an estimate of the error locator polynomial $\gamma \Lambda_E(x)$ (with nonzero $\gamma \in F$) is known, then the polynomial $a^{(i)}(x) \triangleq$

$\psi^{(-1)}(c)$ and/or codeword c for each i can be recovered in many different ways as in Sections V and VI. In the following, we present efficient algorithms for computing $\gamma \Lambda_E(x)$.

B. The SPI Error-Locating Equation

From (108), we obtain

$$\deg(Y^{(i)}(x)\Lambda_E(x) \bmod m(x)) < k^{(i)} + |U_E| \quad (230)$$

for all $i \in \{1, \dots, L\}$.

Lemma 15. Consider a SPI problem as in Section I with $b^{(i)}(x) = Y^{(i)}(x)$, $m^{(i)}(x) = m(x)$, and $\tau^{(i)} = k^{(i)} + |U_E|$ for all $i = 1, \dots, L$; then its solution $\Lambda(x)$ satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k^{(i)} + |U_E| \quad (231)$$

with $\deg \Lambda(x) \leq |U_E|$. \square

Proof: It is immediate from Proposition 1 and (230). \blacksquare

Lemma 16 (SPI Error-Locating Equation). If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (231), then $\Lambda(x)$ is a nonzero polynomial (unique up to a scale factor) of the smallest degree that satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k^{(i)} + \deg \Lambda(x) \quad (232)$$

simultaneously for all $i \in \{1, \dots, L\}$. \square

Proof: Clearly, $\Lambda(x) = \Lambda_E(x)$ satisfies (231) and (232). If some nonzero $\Lambda(x)$ with $\deg \Lambda(x) < |U_E|$ satisfies (232), then it also satisfies (231), which is impossible under the stated assumption. \blacksquare

C. The SPI Error-Locating Algorithm

If $k^{(i)} = k$ for all i , Lemmas 15 and 16 reduce to Lemmas 2 and 3, respectively; in this case, (232) also reduces to (112). Following the same line as in Section VI-B, Lemmas 15 and 16 together suggest the use of Algorithm 4 with $b^{(i)}(x) = Y^{(i)}(x)$, $m^{(i)}(x) = m(x)$, and the adapted

$$\tau^{(i)} = n - 1 - (k_{\max} - k^{(i)}), \quad (233)$$

and $\bar{k}^{(i)} = k^{(i)}$ for all i to compute $\Lambda_E(x)$.

The initialization (233) is made such that in the *very first* check of line 72, the underlying SPI algorithm of Algorithm 4 finds a (nonzero) $\Lambda(x)$ of the smallest degree that satisfies (simultaneously for all i)

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k^{(i)} + d \quad (234)$$

with $d = n - 1 - k_{\max}$. The (common) quantity d will then decrease by one in every later check of line 72.

The error-locating method can be implemented alternatively with Algorithm 5 and/or Algorithm 6, and we have the counterpart of Theorem 4.

Theorem 10. If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (231), then each of Algorithm 4–6 with $b^{(i)}(x) = Y^{(i)}(x)$, $m^{(i)}(x) = m(x)$, $\tau^{(i)} = n - 1 - k_{\max} + k^{(i)}$ as in (233), and $\bar{k}^{(i)} = k^{(i)}$ stops with $\tau^{(i)} \geq k^{(i)} + |U_E|$ and returns $\Lambda(x) = \gamma \Lambda_E(x)$ for some nonzero $\gamma \in F$. \square

Proof: The proof is immediate from Lemma 15, Lemma 16, and the correctness of the underlying SPI algorithm. ■

The justification of Algorithm 4–6 (in this context) hinges on Theorem 12 and Lemma 17 below.

D. Guaranteed Error-Locating Capability

The following Theorem 11, Corollary 2, and Theorem 12, as well as their proofs, are obtained immediately from replacing the respective k in Theorem 9, Corollary 1, and Theorem 5 everywhere by k_{\max} .

Theorem 11. If

$$2|U_E| \leq n - k_{\max} + r_E - 1, \quad (235)$$

then the error locator polynomial (102) satisfies

$$\deg(Y^{(i)}(x)\Lambda_E(x) \bmod m(x)) < \frac{n + k_{\max} + r_E - 1}{2} \quad (236)$$

for all $i \in \{1, \dots, L\}$. Conversely, for any Y and any $E \in F^{L \times n}$ (of rank r_E) and $t \in \mathbb{R}$ with

$$|U_E| \leq t \leq \frac{n - k_{\max} + r_E - 1}{2} \quad (237)$$

if some nonzero $\Lambda(x) \in F[x]$ with $\deg \Lambda(x) \leq t$ satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < n - t + r_E - 1 \quad (238)$$

for all $i \in \{1, \dots, L\}$, then $\Lambda(x)$ is a multiple of $\Lambda_E(x)$. □

Corollary 2. Assume that $2|U_E| \leq n - k_{\max} + r_E - 1$ holds. If some nonzero $\Lambda(x) \in F[x]$ with $\deg \Lambda(x) \leq |U_E|$ satisfies

$$\deg(Y^{(i)}(x)\Lambda(x) \bmod m(x)) < k^{(i)} + |U_E| \quad (239)$$

for all i , then $\Lambda(x) = \gamma\Lambda_E(x)$ for some nonzero $\gamma \in F$. □

In consequence,

Theorem 12 (Sufficient Condition). If

$$2|U_E| < n - k_{\max} + r_E, \quad (240)$$

then $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (231). □

Theorem 12 is a new result that did not appear in the literature, and it improves on Theorem 2 of [8] by a margin of $r_E/2$. If $r_E = |U_E|$, then (240) reduces to

$$|U_E| < n - k_{\max}. \quad (241)$$

E. Statistical Error-Locating Capability

Lemma 17. Let U_E be an arbitrary, but fixed, subset of $\{0, \dots, n-1\}$, and assume that the $|U_E|$ nonzero columns of the $L \times n$ matrix E are uniformly and independently distributed over $F^L \setminus \{0\}$. Then the probability P_Λ that $\Lambda(x) = \Lambda_E(x)$ does not solve the SPI problem (231) is bounded by

$$P_\Lambda < \frac{q^{-L(n-k_{\text{avg}})+(L+1)|U_E|}}{q-1} \quad (242)$$

for $L > 1$. □

The proof is given below.

Theorem 13 (Probability of Decoding Failure). Assume

$$\frac{L}{L+1}(n - k_{\text{avg}}) < n - k_{\max} \quad (243)$$

and $L > 1$. If the $|U_E|$ nonzero columns of the error pattern are uniformly distributed over $F_q^L \setminus \{0\}$, then the probability P_f that (any of) Algorithm 4–6 fails is bounded by

$$P_f < \frac{q^{-L(n-k_{\text{avg}})+(L+1)|U_E|}}{q-1} \quad (244)$$

□

Proof: By Lemma 17 and $P_f \leq P_\Lambda$. ■

Note that (244) implies that errors can be corrected (with high probability, if q is large) up to the radius

$$\frac{L}{L+1}(n - k_{\text{avg}}). \quad (245)$$

In the special case where $k^{(i)} = k$ for all i , (245) reduces to (121), and in this case, (243) is automatic.

We now prove Lemma 17.

Proof of Lemma 17: Recall the polynomial $E^{(i)}(x)$ from (100). The proof starts with the following fact:

Proposition 11. If $\Lambda(x) = \Lambda_E(x)$ does not solve the SPI problem (231), then there exists some nonzero polynomial $\Lambda(x)$ such that $\deg \Lambda(x) < |U_E|$ and

$$\deg(E^{(i)}(x)\Lambda(x) \bmod m(x)) < k^{(i)} + |U_E| \quad (246)$$

for all $i = 1, \dots, L$. □

For simplicity, we denote below U_E by U , and $|U_E|$ by $|U|$.

Let S_U be the set of all the possible error matrices E with the given support set U . Let $S_f \subset S_U$ be the set of all $E \in S_U$ that admit some $\Lambda(x) \in F[x]$ with $0 \leq \deg \Lambda(x) < |U|$ that satisfies (246) for all $i \in \{1, \dots, L\}$. Then

$$P_\Lambda \leq \frac{|S_f|}{|S_U|} = \frac{|S_f|}{(q^L - 1)^{|U|}} \quad (247)$$

It thus remains to bound $|S_f|$.

For $t = 0, \dots, |U| - 1$, let \mathcal{L}_t be the set of monic polynomials $\Lambda(x) \in F[x]$ with $\deg \Lambda(x) < |U|$ and with exactly t zeros in the set $\mathcal{B}_U \triangleq \{\beta_\ell : \ell \in U\}$.

Lemma 18. For any fixed $\Lambda(x) \in \mathcal{L}_t$, the number of error patterns $E \in S_U$ that satisfy (246) is upper bounded by $q^{L(2|U|-(n-k_{\text{avg}})-t)}$. □

Proof of Lemma 18: Consider the polynomial $E^{(i)}(x) = \psi^{-1}(e^{(i)})$ where $e^{(i)}$ is a row of E , and let $\tilde{E}^{(i)}(x) \triangleq E^{(i)}(x)\Lambda(x) \bmod m(x)$. From (96), we have

$$\tilde{E}^{(i)}(\beta_\ell) = e_{i,\ell}\Lambda(\beta_\ell) \quad (248)$$

where $e_{i,\ell}$ denotes the element in row i and column ℓ of E . From (246), we have $\deg \tilde{E}^{(i)}(x) < k^{(i)} + |U|$. But (248) implies that $\tilde{E}^{(i)}(x)$ has at least $n - |U| + t$ zeros in prescribed positions: $e_{i,\ell} = 0$ for $\ell \notin U$ and $\Lambda(x)$ has t zeros in $\mathcal{B}_U = \{\beta_\ell : \ell \in U\}$. By Proposition 9, the number of such polynomials $\tilde{E}^{(i)}$ is bounded by $q^{2|U|-(n-k^{(i)})-t}$, and putting all rows together yields the lemma. □

We then have

$$|S_f| \leq \sum_{t=0}^{|U|-1} |\mathcal{L}_t| q^{L(2|U|-(n-k_{\text{avg}})-t)}. \quad (249)$$

Recall from Lemma 10 that

$$|\mathcal{L}_t| = \binom{|U|}{t} (q-1)^{|U|-t-1}. \quad (250)$$

Thus (249) becomes

$$|S_f| \leq \sum_{t=0}^{|U|-1} \binom{|U|}{t} (q-1)^{|U|-t-1} q^{L(2|U|-(n-k_{\text{avg}})-t)} \quad (251)$$

$$= w \sum_{t=0}^{|U|-1} \binom{|U|}{t} (q-1)^{-t} q^{-Lt} \quad (252)$$

$$< w \sum_{t=0}^{|U|} \binom{|U|}{t} ((q-1)^{-1} q^{-L})^t \quad (253)$$

$$= w (1 + (q-1)^{-1} q^{-L})^{|U|} \quad (254)$$

$$= \frac{q^{L(|U|-(n-k_{\text{avg}}))}}{q-1} ((q-1)q^L + 1)^{|U|} \quad (255)$$

with

$$w \triangleq (q-1)^{|U|-1} q^{L(2|U|-(n-k_{\text{avg}}))} \quad (256)$$

in (252)–(254). From (247), we then have

$$P_f < \frac{q^{L(|U|-(n-k_{\text{avg}}))}}{q-1} \left(\frac{q^{L+1} - q^L + 1}{q^L - 1} \right)^{|U|} \quad (257)$$

$$= \frac{q^{-L(n-k_{\text{avg}}-|U|)+|U|}}{q-1} \left(\frac{q^L - (q^{L-1} - q^{-1})}{q^L - 1} \right)^{|U|} \quad (258)$$

and (242) follows if $L > 1$. \square

F. A Remark on the SPI Problem (231)

In contrast to (240), the bound (245) is a *necessary* condition for $\Lambda_E(x)$ to solve the SPI problem (231): by Proposition 3, if $\Lambda_E(x)$ solves the SPI problem (231), then

$$|U_E| \leq \sum_{i=1}^L (n - k^{(i)} - |U_E|), \quad (259)$$

which yields (245).

G. The Reduced SPI Error-Locating Algorithm

If $\Lambda_E(x)$ solves the SPI problem (231), then from (22), coefficients $Y_\ell^{(i)}$ of $Y^{(i)}(x)$ for

$$\begin{aligned} \ell &< k^{(i)} + |U_E| - \sum_{i=1}^L (n - k^{(i)} - |U_E|) \\ &\leq k^{(i)} \end{aligned}$$

(where the last step is easily seen from (259)) are irrelevant and can be set to zero. We then obtain the counterpart of Lemma 5.

Lemma 19 (Reduced SPI Problem).

Let

$$\tilde{Y}^{(i)}(x) \triangleq Y^{(i)}(x) \operatorname{div} x^{k^{(i)}} \quad (260)$$

and

$$\tilde{m}^{(i)}(x) \triangleq m(x) \operatorname{div} x^{k^{(i)}} \quad (261)$$

for $i = 1, \dots, L$. Then $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (231) if and only if it solves the SPI problem

$$\deg(\tilde{Y}^{(i)}(x)\Lambda(x) \bmod \tilde{m}^{(i)}(x)) < |U_E|. \quad (262) \quad \square$$

Lemma 20 (Reduced SPI Error-Locating Equation). If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (262), then $\Lambda(x)$ is a nonzero polynomial of the smallest degree (unique up to a scale factor) that satisfies

$$\deg(\tilde{Y}^{(i)}(x)\Lambda(x) \bmod \tilde{m}^{(i)}(x)) < \deg \Lambda(x) \quad (263)$$

simultaneously for all $i \in \{1, \dots, L\}$. \square

Then from the equivalence of the SPI problems (231) and (262), and the correspondence between Lemmas 16 and 20, we obtain the analog of Theorem 10.

Theorem 14. If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (262), then each of Algorithm 4–6 with $b^{(i)}(x) = \tilde{Y}^{(i)}(x)$, $m^{(i)}(x) = \tilde{m}^{(i)}(x)$, $\tau^{(i)} = \deg m^{(i)} - 1 - (k_{\max} - k^{(i)})$, and $\bar{k}^{(i)} = 0$ stops with $\tau^{(i)} \geq |U_E|$ and returns $\Lambda(x) = \gamma \Lambda_E(x)$ for some nonzero $\gamma \in F$. \square

In the special case where $k^{(i)} = k$ for all i , Theorem 14 reduces to Theorem 7.

H. Monomialized SPI Error-Locating Equation

The SPI problem (231) for general $m(x)$ can be transformed into another SPI problem as follows.

Lemma 21 (Monomialized SPI Problem). For $b^{(i)}(x) = Y^{(i)}(x)$ and $m^{(i)}(x) = m(x)$, let $\tilde{b}^{(i)}(x)$ be the polynomial (40) with $n^{(i)} \triangleq n$, $\tau^{(i)} = k^{(i)} + |U_E|$, and $u \triangleq |U_E|$ for $i = 1, \dots, L$. Then $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (231) if and only if it solves the SPI problem

$$\deg(\tilde{b}^{(i)}(x)\Lambda(x) \bmod x^{n-k^{(i)}}) < |U_E|. \quad (264) \quad \square$$

Proof: It is immediate from Theorem 1. \blacksquare

Lemma 22 (Monomialized SPI Error-Locating Equation). If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (264), then $\Lambda(x)$ is a nonzero polynomial of the smallest degree (unique up to a scale factor) that satisfies

$$\deg(\tilde{b}^{(i)}(x)\Lambda(x) \bmod x^{n-k^{(i)}}) < \deg \Lambda(x) \quad (265)$$

simultaneously for all $i \in \{1, \dots, L\}$. \square

The proof is an obvious adaption of the proof of Lemma 16.

By Lemmas 19 and 21, the two SPI problems (262) and (264) are equivalent. Then from the correspondence between Lemmas 20 and 8, we have

Theorem 15. If $\Lambda(x) = \Lambda_E(x)$ solves the SPI problem (264), then each of Algorithms 4–6 with $b^{(i)}(x) = \tilde{b}^{(i)}(x)$, $m^{(i)}(x) = x^{n-k^{(i)}}$, $\tau^{(i)} = \deg m^{(i)} - 1 - (k_{\max} - k^{(i)})$, and $\bar{k}^{(i)} = 0$ stops with $\tau^{(i)} \geq |U_E|$ and returns $\Lambda(x) = \gamma \Lambda_E(x)$ for some nonzero $\gamma \in F$. \square

REFERENCES

- [1] J.-H. Yu and H.-A. Loeliger, "An algorithm for simultaneous partial inverses," *Proc. 52th Annu. Allerton Conf. Commun. Control, and Comput.*, Monticello, IL, USA, Oct. 2014, pp. 928–935.
- [2] J.-H. Yu and H.-A. Loeliger, "Decoding of interleaved Reed-Solomon codes via simultaneous partial inverses," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, China, June 2015, pp. 2396–2400.
- [3] J.-H. Yu and H.-A. Loeliger, "Reverse Berlekamp-Massey decoding," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, July 2013, pp. 1212–1216.
- [4] J.-H. Yu and H.-A. Loeliger, "Partial inverses mod $m(x)$ and reverse Berlekamp-Massey decoding," *IEEE Trans. Inf. Theory*, vol. 62, No. 12, pp. 6737–6756, Dec. 2016.
- [5] G.-L. Feng and K. K. Tzeng, "A generalized Euclidean algorithm for multi-sequence shift-register synthesis," *IEEE Trans. Inf. Theory*, vol. 35, pp. 584–594, May 1989.
- [6] G.-L. Feng and K. K. Tzeng, "A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes," *IEEE Trans. Inf. Theory*, vol. 37, pp. 1274–1287, Sept. 1991.
- [7] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding of interleaved Reed-Solomon codes over noisy data," *Lect. Notes Computer Sci.*, vol. 2719, pp. 97–108, 2003.
- [8] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Collaborative decoding of interleaved Reed-Solomon codes and concatenated codes designs," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2991–3012, July 2009.
- [9] J. S. R. Nielsen, "Generalized multi-sequence shift-register synthesis using module minimisation," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, July 7–12, 2013.
- [10] R. M. Roth and P. O. Vontobel, "Coding for combined block-symbol error correction," *IEEE Trans. Inf. Theory*, vol. 60, pp. 2697–2713, May 2014.
- [11] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. 15, No. 1, pp. 122–127, May 1969.
- [12] A. Brown, L. Minder, and M. A. Shokrollahi, "Probabilistic decoding of interleaved RS-codes on the Q -ary symmetric channel," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Chicago, USA, June 27–July 2, 2004.
- [13] F. Parvaresh and A. Vardy, "On the performance of multivariate interpolation decoding of Reed-Solomon codes," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, USA, July 9–14, 2006.
- [14] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon codes and algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1755–1764, Sept. 1999.
- [15] F. Parvaresh and A. Vardy, "Multivariate interpolation decoding beyond the Guruswami-Sudan radius," *Proc. 42th Annu. Allerton Conf. Commun. Control, and Comput.*, Urbana, Illinois, USA, October, 2004.
- [16] J. J. Metzner and E. J. Kapturowski, "A general decoding technique applicable to replicated file disagreement location and concatenated code decoding," *IEEE Trans. Inf. Theory*, vol. 36, pp. 911–917, July 1990.
- [17] C. Haslach and A. J. H. Vinck, "A decoding algorithm with restrictions for array codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2339–2344, Nov. 1999 (and correction in the same publication, vol. 47, p. 470, Jan. 2001).
- [18] H. Kurzweil, M. Seidl, and J. B. Huber, "Reduced-complexity collaborative decoding of interleaved Reed-Solomon and Gabidulin codes," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Saint Petersburg, Russia, July 31–Aug. 5, 2011.
- [19] G. Schmidt and V. R. Sidorenko, "Multi-sequence linear shift-register synthesis: the varying length case," *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, Seattle, USA, July 9–14, 2006.
- [20] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Decoding Reed-Solomon codes beyond half the minimum distance using shift-register synthesis," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, USA, July 9–14, 2006.
- [21] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge University Press, Cambridge, UK, 2003.
- [22] J.-H. Yu and H.-A. Loeliger, "On irreducible polynomial remainder codes," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Saint Petersburg, Russia, July 31–Aug. 5, 2011.
- [23] J.-H. Yu and H.-A. Loeliger, "On polynomial remainder codes," <http://arxiv.org/abs/1201.1812>.